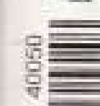
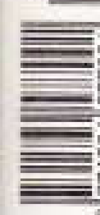
www.hackerjournal.it N. 50



IMPERDIBILE!

HJ NUMERO 50 DA COLLEZIONE





2 €
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

Ascolti proibiti
con una radio FM

NON DIGITARE SULLA TASTIERA
keylogger in ascolto!

L'ultima FREGATURA MICROSOFT

Ci mette più di SEI MESI a correggere un BUG!

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."



Anno 3 – N. 50
6/20 Maggio 2004

Direttore Responsabile: Luca Sprea

I Ragazzi della redazione europea:
Bismark.it, Il Coccia, Gualtiero Tronconi, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron
Contents by MDR

Service: Cometa s.a.s.

DTP: Davide "Fo" Colombo

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Daniele Festa

Publishing company:
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing:
Roto 3

Distributore:
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti:
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Pubblicazione quattordicinale registrata al Tribunale di Milano
il 27/10/03 con il numero 601.

editoriale

HJ numero 50!

Personalmente non amo troppo le autocelebrazioni e cose simili, e questo mini-anniversario stava per sfuggirmi, preso dalla quotidianità degli impegni. Però qualche giorno fa mi sono fermato un attimo e mi sono detto: "Ma siamo davvero al numero 50?". Accipicchia! Ammetto che è un bel risultato :-) e gongolo fra me e me, pensando che all'inizio, in fondo, non molti sarebbero stati disposti a scommettere che saremmo arrivati fin qui. L'hacking sembrava (ad alcuni) più un fenomeno di moda che un movimento culturale con basi profonde e destinato a durare. E infatti siamo ancora qui, con ancora più voglia di quando siamo partiti, con più esperienza, e con la stessa curiosità verso tutto ciò che ci circonda e che ci spinge a volerne sapere di più. Un po' curiosi e un po' impiccioni, insomma...



Numero 50, copertina bianca (la prima!), 49 copertine con un teschio, 1600 pagine pubblicate fin qui, centinaia di news, articoli, inchieste, non so più quante righe di codice studiate, una marea di pagine Web messe on-line, migliaia e migliaia di mail lette (tutte!), zero pagine di pubblicità.

Il ringraziamento sincero - e non di rito - va a tutti quelli che hanno contribuito in questi mesi a realizzare 50 numeri.

Da Grand, a Il Coccia, a Bismark, a Cometa, a tutti i collaboratori (troppi per nominarli tutti), ai moderatori del forum (karmageddon fra tutti), a Silvia, ai grafici che sono stati dietro ai nostri capricci estetici, a Daniele per le copertine, a Lidia e Gualtiero per il lavoro di segreteria, agli edicolanti e non ultimo all'editore. Ma soprattutto vorrei ringraziare tutti i lettori che ci hanno seguito numero dopo numero senza mai stancarsi di scriverci, di postare sul nostro forum, di venirci a trovare a SMAU, dandoci sempre la sensazione di non essere soli a "cucinare" queste pagine.

TheGuilty@hackerjournal.it

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. redazione@hackerjournal.it

HACKER JOURNAL

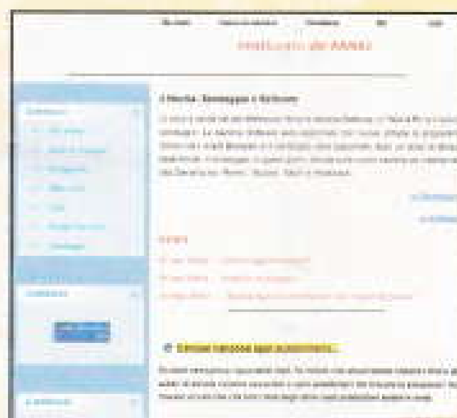
La prima rivista hacking italiana

88mhz

Vi prego di pubblicare il mio sito.
http://www.88mhz.net
Parla di modding, di computer, di download e di altro...
Vi prego...

Ciao
Aurelio M.

Grazie a te della segnalazione! Ci piace la... frequenza con cui arrivano.



Versi virali

(Virus Dona *)*

Ormai libera
hai spezzato le catene.
Nessuna legge
di questo sistema è per te.
Ora tu
urli idee nuove
e pulite
mentre il sistema ti "arresta"
per la libertà che ti sei concessa.

P.S. Una poesia dedicata ad ogni programma "ribelle" come me e come voi!

by blackhole #0

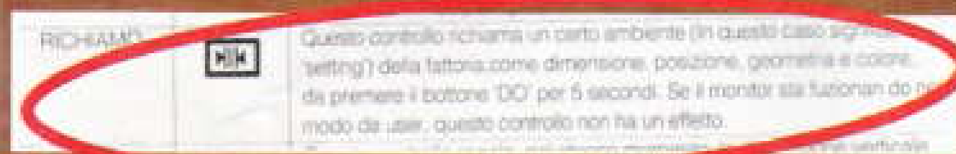
Ribelli sempre, e sempre "per" la conoscenza, mai "contro"...

Benvenuti in Fattoria!

Ciao a tutti,
vi invio in allegato un particolare del manuale del mio monitor Hansol.

Invece di scrivere "Impostazioni di fabbrica" hanno scritto "Impostazioni di FATTORIA".
Grazie per l'attenzione.

MikispagMonitor da periti agrari, quelli con le impostazioni di fattoria...



RICHIAMO — Questo controllo richiama un certo ambiente (in questo caso significa "setting") della fattoria come dimensione, posizione, geometria e colore. da premere il bottone 'DO' per 5 secondi. Se il monitor sta funzionando ne modo da user, questo controllo non ha un effetto.

Portale a portale

Salve a tutta la redazione di HJ, volevamo segnalarvi il nuovo portale informatico che abbiamo creato...
http://www.overclokkati.com/

FrancescoFra & PuMaX



Teste di Hacker!

Volevo segnalare il mio sito:
http://www.hackermind.tk
È ancora giovane ma promette bene!!!

Bonny

Il cervello sembra già ben sviluppato, radiografie alla mano!



SECRETZONE

Nuova Password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troveremo arretrati, sfondi, informazioni e approfondimenti interessanti. Con alcuni browser, può capitare di dover inserire due volte gli stessi codici. Non fermiamoci al primo tentativo!

USER: PUPIS

PASS: SIPUP

SEDICENNE CHE DIVENTERÀ

Sono uno di quei tanti (troppi!) sedicenni che si credono grandi hacker, ma che non riescono a cavare un ragno dal buco senza la vostra rivista in mano. Non mi definisco e non amo farmi definire hacker. I veri hacker sono là fuori e fanno cose che io non potrei nemmeno immaginare. Sono un sedicenne che si interessa un po' troppo di sicurezza informatica, null'altro. Ho letto i vostri articoli sull'installazione di Linux su Xbox.



Sono un fortunato possessore della console Sony (perché piuttosto che dare altri soldi allo Zio Bill avrei fatto follie, ho già messo troppo a repentaglio la mia privacy usando WinXp), la mitica PlayStation2, e mi chiedevo se esistesse la possibilità di installare una versione di Linux (o una versione Live, dato che l'HardDisk per PlayStation2 non è ancora disponibile in Europa) sulla mia PlayStation2. Ero interessato al fatto di potere vedere la rete tra un gioco e l'altro e magari dare anche un'occhiata alla mia casella email, con l'apposito adattatore di rete.

Nicolò

Ciao Nicolò!
A noi risulta che l'hard disk per Playstation sia perfettamente disponibile in Europa, a linuxplay.com. Controlla e facci sapere. Complimenti a te per i tuoi sedici anni invece; sei sveglio, intelligente e pronto a imparare un sacco di cose. Sei più hacker tu che tanti script kiddy capaci solo di lanciare roba già fatta da altri.

LA FINANZA DAVANTI A CASA

Solo per curiosità, se si compie un atto illegale con i peer to peer, quanto tempo ci vuole prima che si venga a sapere di "essere stati scoperti"? Tengo a sottolineare, solo x curiosità!

supercomputer

Non è che ti avvisano con raccomandata espresso! Sempre parlando per ipotesi, naturalmente, se ti suona la Finanza a casa vuol dire che ti hanno scoperto sì. Altrimenti si tengono l'asso in mano e aspettano di giocarlo. Già che ci siamo; la Finanza effettua ispezioni anche in case private. Tuttavia si concentra su chi la fa grossa, tipo mettere su server pieni di giochi commerciali, o comunque fa troppo traffico. Come dimostrano le vicende del decreto Urbani, chi scarica musica a uso personale in modo ragionevole non corre di fatto rischi. Se poi scarica solo materiale scaricabile, tanto meglio.



▲ ***No, non ti avvisano prima di venire a suonare a casa tua. Se vuoi offrire il caffè, devi fare provvista.***

IL GIORNO DEL GIUDIZIO DOPO

[In riferimento all'articolo sull'algoritmo del Giorno del Giudizio per sapere a memoria in che giorno della settimana cade qualunque data, pubblicato sul numero 46, N.d.B] Per gli anni che sono secoli, solo quelli divisibili per 400 sono bisestili, dunque non il 1900. Ogni 12 anni il GdG avanza di un giorno solo se in questi 12 anni non è presente un secolo come il 1900 suddetto. Per le date precedenti al 15 ottobre 1582 si deve ricordare il cambio dal calendario giuliano al calendario gregoriano odierno che soppresse 10 giorni passando dal 4 ottobre 1582 direttamente al 15 ottobre 1582. Prima di tale data erano bisestili tutti gli anni divisibili per 4 (per lo meno suppongo dall'introduzione del calendario giuliano). Il metodo proposto dunque dovrebbe funzionare solo dal 1901 al 2099 (il 2100 a sua volta non sarà bisestile, mentre per fortuna il 2000 lo è stato).



Fabio Tagliabracci

Lo spazio a disposizione non consentiva di approfondire ma il metodo funziona anche per gli altri secoli, a condizione di tenere conto della tua osservazione (che è corretta) e applicare un modificatore relativamente semplice.
Gli anni di fine secolo, infatti, hanno tutti un Giorno del Giudizio (GdG) ciclico su quattrocento anni:

Domenica = 1700, 2100, 2500...
Martedì = 1600, 2000, 2400...
Mercoledì = 1500, 1900, 2300...
Venerdì = 1800, 2200, 2600...

È dunque relativamente facile tenere conto anche dei secoli fino al 1600 e quelli futuri.
Per le date prima del 1582 bisogna effettivamente modificare il calcolo secondo quanto lei giustamente riporta.

CANCELLAZIONE SICURA DATI

Sono un vostro lettore utente Mac; cosa ne pensate dell'opzione "Vuota cestino sicuro" supportata dal sistema operativo Mac OS X 10.3.3, nome in codice Panther? Una volta eliminati i dati con questa opzione, sono ancora recuperabili? Certo non è una soluzione veloce da adottare all'ultimo minuto in caso di emergenza, ma mi piacerebbe sapere se è efficace.

Dino Ferrari

Lo svuotamento sicuro del Cestino in Mac OS X 10.3 riscrive i settori del disco che ospitavano i dati per un certo numero di volte. Quei dati saranno certamente irrecuperabili dalle utility ordinarie. Forse (forse) un laboratorio specializzato, spendendo molto, potrebbe ritrovarli.



LYX È QUI

Vorrei sapere dove posso recuperare LyX, l'elaboratore di documenti di cui avete parlato nella rivista, per Windows XP.

Vari lettori

LyX per Windows si trova per esempio a http://www.home.zonnet.nl/rareitsma/lyx/ e ha bisogno, per funzionare, di LaTeX. Per quest'ultimo esiste una buona versione di LaTeX per Windows di nome MidTeX, a http://www.midtex.org/. Sia LyX che LaTeX sono inoltre stati inseriti nel CD-ROM di Hackers Magazine numero 17 e numero 18.



DOVE STA WIKIPEDIA

Ho sentito parlare di un'enciclopedia open source di nome Wikipedia e vorrei sapere dove poterla scaricare.

Massimiliano

Wikipedia in italiano sta all'indirizzo http://it.wikipedia.org e quella in inglese sta a http://www.wikipedia.org. Esiste in un sacco di altre lingue, ma trovi facilmente i link sul sito. Più che altro Wikipedia è da consultare. Se vuoi veramente scaricarla avrai bisogno di pazienza, perché consta di oltre mezzo milione di pagine Web!

PER DAVIA



LIBRI IN SCONTO

Ho letto sulla rivista la risposta che riguarda i libri Hacker all'attacco e Manuale del giovane hacker; il secondo l'ho trovato nel vostro sito, ma il primo no.

adrians

Ti basta partire dal link che hai trovato e, arrivato sul sito Hops Libri, caricare la pagina dell'altro libro. Continui ad avere lo sconto e lo hai su tutti i libri del catalogo online. Se hai difficoltà, parti da http://www.hopslibri.com/cgi-bin/hops?mv_pc=hj e clicca su "catalogo_on_line".



▲ ***I lettori di Hacker Journal hanno lo sconto del 15 percento sull'acquisto online dei titoli di Hops Libri.***

HOT!

LASER E PC SBANCANO LA ROULETTE

Al casinò dell'hotel Ritz di Londra tre scommettitori-hacker, armati di tecnologia, hanno vinto oltre due milioni di euro e il bello che potrebbero avere fatto tutto in perfetta legalità. Il trio, due serbi e una ungherese, ha usato uno scanner nascosto in un cellulare a sua volta collegato a un computer. Il meccanismo riesce a calcolare la velocità della pallina tra il primo e il terzo colpo assestato alla ruota della roulette dal croupier, prima che venga pronunciata la fatidica frase "Les jeux son fait, rien ne va plus" che chiude le giocate. Il computer elabora rapidamente la probabile casella di arresto della pallina e comunica l'informazione ai giocatori. Scotland Yard ha voluto comprensibilmente saperne di più ma il sistema potrebbe essere regolare. Infatti il laser non influisce in alcun modo sulla roulette ma si limita a leggerne le condizioni e quindi non falsa il gioco, che si svolge in modo del tutto regolare. Se passerà la liceità della vincita ai casinò di tutto il mondo gireranno davvero le palline.



WITTY DISTRUGGI COMPUTER



Piccolissimo (è scritto in linguaggio assembly) e cattivissimo, Witty è uno dei worm più recenti che affliggono i computer Windows. Come Blaster non ha bisogno di essere eseguito ma si installa attraverso un punto debole comune a certi programmi della Internet Security Systems (ISS, http://www.iss.net/), che produce tra l'altro il firewall Black Ice.
Uno dei componenti di questi programmi, il Protocol Analysis Module o PAM, è vulnerabile quando analizza il traffico generato dal protocollo usato da ICQ per le chat e Witty ne approfitta, infiltrandosi nella macchina vittima e inviando pacchetti UDP dalla porta 4000 verso ventimila indirizzi IP casuali. In più danneggia l'hard disk in modo tale che va riformattato. Il sito di ISS contiene l'elenco di tutti i programmi affetti e soprattutto le patch per tappare le falle.

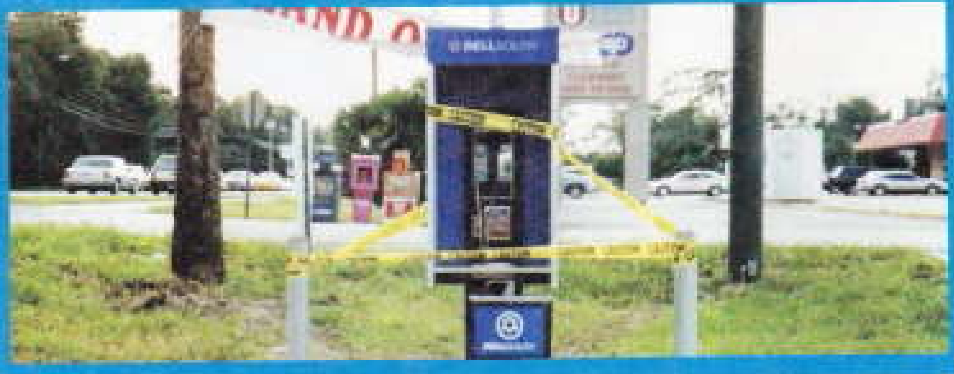
FINTO AVVISO MICROSOFT

Capita che arrivi in posta un messaggio che sembra inviato da Microsoft, con mittente tipo help@microsoft.com o alert@microsoft.com, ad avvisare che è in circolazione una ennesima variante del virus (ma anche worm) Mydoom.
Il messaggio contiene un allegato che, secondo il messaggio, sarebbe un aggiornamento contro il virus. In realtà il messaggio è falso, l'allegato è un virus e il mittente ovviamente non ha Microsoft. Che ha un sacco di difetti ma, sicuramente, non invia mai aggiornamenti via posta elettronica.



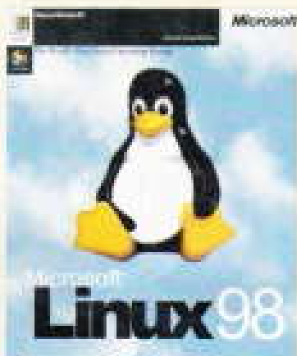
ALLEGATO? NO, GRAZIE!

Nel mondo c'è un'infinità di macchine Windows non aggiornate all'ultimissima patch antivirus e tra i tanti colabrodi c'è anche quello che riesce a prendere un virus tramite una mail priva di allegato. Lo specialista di questo sport si chiama Bagle.Q, che sfrutta la centomiliardesima vulnerabilità di Internet Explorer. Bagle.Q invia una mail senza allegato, ma in formato HTML, con dentro un link al virus, che attende su un sito. Su una macchina non aggiornata l'HTML lancia uno script in Visual Basic e va a scaricare da solo il virus. Ovviamente basta usare un browser diverso da Explorer per non correre alcun rischio. Ma c'è chi ama il brivido...



ATTENTI AL BIZEX

A qualcuno è arrivato un messaggio ICQ che invita a visitare il sito Jokeworld. Se proprio vogliamo andare a vedere il sito, che in realtà è un'esca, con Explorer, facciamolo con una copia aggiornata. Se non lo è il virus di nome Bizex si installa, in modo anche abbastanza ingegnoso. La pagina-esca, infatti, cambia il file STARTUP.WAV di ICQ con un file contenente uno script il quale, eseguito, crea un file WINUPDATE.EXE. Quest'ultimo, appena eseguito, preleva da Internet ed esegue un file APTGETUPD.EXE, che è il nucleo del virus. A questo punto il file si trasferisce sotto il nome di SYSMON.EXE in una sottocartella di \System, installa un programmino che ascolta quanto viene battuto sulla tastiera alla ricerca di dati sensibili (numeri di carte di credito?) e tenta di contattare via ICQ tutti i contatti della vittima per ripetere il giochetto. Basta usare un browser diverso da Explorer per non avere alcun problema.



ALL'ATTACCO DEI SET-TOP BOX

David Jeansonne, 43 anni, americano della Lousiana, è stato arrestato dall'FBI per avere sabotato le utenze di alcuni abbonati a MSN TV. Questa rete nasce dalle ceneri di WebTV e funziona tramite set-top box che consentono di navigare e ricevere posta dal televisore di casa. Jeansonne ha messo a punto uno script che apparentemente permetteva di cambiare i colori dell'interfaccia utente e intanto cambiava le impostazioni del modem in modo che chiamasse il 911 (il nostro 113 di emergenza). Lo ha mandato a 18 utenti, alcuni dei quali lo hanno passato a colleghi e amici facendo ancora meglio dello script, incapace di replicarsi di suo.
Il pirata del set-top box è uscito su cauzione (25 mila dollari) e adesso attende il giudizio. È il futuro che attende il nostro digitale terrestre?



A MESSA IN 3D

Chi avrebbe mai pensato che fosse possibile realizzare una Chiesa virtuale? È nata. Si chiama Church of Fools, la Chiesa dei folli, e partirà l'11 maggio, per durare tre mesi in un esperimento davvero bizzarro. Le funzioni sono tenute veramente da autentici pastori, che vengono raffigurati con avatar appositi all'interno di un ambiente 3D accessibile online da parte dei fedeli. Anche questi ultimi avranno il loro posto in "parrocchia" e ci sarà persino la raccolta delle offerte, sotto forma di SMS inviati a un numero apposito. I partecipanti alla messa online potranno solo ascoltare, ma a fine funzione saranno liberi di chattare tra loro. Diciamo la verità: se funziona, è un... miracolo.



HOT!

IL GRANDE CONTROLLORE

Trenitalia si avvia a installare a titolo sperimentale in Piemonte su quaranta treni regionali telecamere per la videosorveglianza. La motivazione è naturalmente quella della sicurezza dei viaggiatori, ma resta il fatto che chiunque viaggerà in treno per quelle zone verrà filmato, sia che entri nella toilette quando il treno è fermo in stazione sia che legga un giornaletto sexy sia che si schiacci un punto nero. Che dire? Dal Grande Fratello al Grande Controllore.



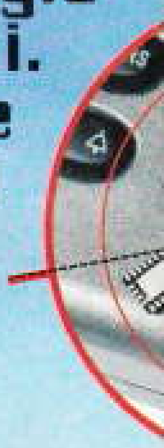
ITUNES? NO, GRAZIE

Vogliamo acquistare musica dall'iTunes Music Store senza bisogno di usare iTunes? Non c'è problema! Basta usare l'interfaccia Web iTMS-4-ALL ospitata dal gruppo di Downhill Battle a http://www.downhillbattle.org/cgi-bin/itms4all.pl, con qualsiasi browser. Ne parliamo in un prossimo numero più approfonditamente anche dal punto di vista tecnico; per ora basti dire che iTunes non è più un obbligo, e tanto basti. Domani potrebbe nascere un client iTunes per Linux, o mille altre possibilità.



TERRORISTI

Usavano il telefonino con le schede dalla Svizzera, ma la tecnologia li ha incastrati. Una lezione esemplare!



L'operazione Mont Blanc è cominciata quasi per caso nell'aprile 2002, quando le autorità svizzere intercettarono una chiamata lunga meno di un minuto, interamente silenziosa. L'11 settembre era ancora fin troppo recente e gli inquirenti si chiesero se quella chiamata non fosse per caso un segnale convenuto tra terroristi. Lo era. L'operazione è durata quasi due anni e ha portato alla scoperta e allo smantellamento di cellule del terrore in tre diversi continenti. Con un unico denominatore: il cellulare a scheda. Che non è sicuro, anche se non c'è dietro un contratto. Una delle presunte menti dell'11 settembre, Khalid Shaikh Mohammed, è la vittima più eccellente dell'operazione. È stato arrestato a marzo in Pakistan. Il tutto è in gran parte frutto delle intercettazioni telefoniche compiute sui cellulari dei sospetti, e su un clamoroso errore di valutazione di questi ultimi. Che avevano acquistato numerose schede telefoniche di Swisscom, preferite

BIN LADEN E I MESSAGGINI



Durante i bombardamenti su Tora Bora in Afghanistan del dicembre 2001, le autorità americane hanno riferito di avere ascoltato Osama bin Laden parlare con i suoi contatti tramite un telefono satellitare. Ora, ammesso che sia ancora vivo, preferisce comunicare attraverso bigliettini di carta trasportati da corrieri fidati.



INCASTRATI DAL CELLULARE

perché potevano essere comprate senza neanche fornire un nome, ancorché falso, e permettevano di chiamare da tutto il mondo. L'investigazione è partita dalla Svizzera e ha coinvolto oltre una decina di Paesi tra i quali l'Italia, gli Stati Uniti, Pakistan, Arabia Saudita, Germania e Gran Bretagna. La chiamata che ha dato inizio a tutto è avvenuta l'11 aprile 2002, quando Christian Ganczarski, musulmano polacco trentaseienne nato in Germania e sospettato di legami con Al Qaida, ha composto il numero di Khalid Shaikh Mohammed, in quel momento al sicuro nella sua abitazione in Pakistan.

La chiamata doveva avvisare Mohammed di un attentato suicida in una sinagoga tunisina, avvenuto il giorno stesso e costato la vita a 21 persone, quasi tutte turisti tedeschi.
Due settimane dopo l'attentato la polizia effettuò una perquisizione a casa Ganczarski trovando un elenco di numeri cellulari, compreso quello intercettato, che portava diritto a Mohammed. Indagini successive portarono alla scoperta della predilezione dei terroristi per le schede Subscriber Identity Module Cards prodotte da Swisscom. L'errore di Mohammed? Usava moltissimi telefoni, tanto che le autorità non arrivano a individuarne subito la posizione, ma insisteva a usare sempre la stessa SIM.

L'arresto di Mohammed ha portato alla scoperta di altre centinaia di numeri telefonici, oltre a computer e numerosi cellulari. A catena, i numeri scoperti hanno portato a rilevare più di seimila contatti telefonici, in pratica disegnando una mappa virtuale delle comunicazioni di Al Qaida.

Ora l'operazione Mont Blanc ha prodotto tutti i risultati che poteva dare e si è virtualmente conclusa, anche se le autorità terrebbero sotto controllo ancora un numero limitato di schede. Nel frattempo, il primo luglio 2004 entrerà in vigore in Svizzera una legge che vieta l'acquisto di schede per cellulari a meno che l'acquirente non fornisca un minimo di informazioni personali.

L'operazione Mont Blanc ha probabilmente reso le nostre vite più sicure. Ma ha confermato che le nostre comunicazioni non lo sono affatto.

NeOkOn
neOkOn@hacker journal.it

◁ Per le autorità impegnate nella lotta al terrorismo le SIM Swisscom usate da Al Qaida non avevano prezzo.



Tutte le immagini sono fornite da Global Locate, Inc.

THE BIG GUY



Nel giugno 2003, tra le centinaia di telefonate intercettate nel corso dell'operazione Mont Blanc, una diceva "sta arrivando il pezzo grosso. Sarà qui presto". Il pezzo grosso si è rivelato essere Abdullah Oweis, arabo saudita, perno dell'organizzazione di Al Qaida, a suo agio tra gli occidentali quanto tra i mujahiddin. Oweis è stato arrestato in Qatar lo scorso luglio.



△ Dopo l'11 settembre l'attività di intercettazione telefonica è cresciuta a dismisura in tutto il mondo. Qui si vede un momento successivo all'impatto contro il Pentagono di uno degli aerei dirottati.

AL-ZARKAWI E LE CHIAMATE IN CODICE

Nel 2002 le autorità tedesche hanno intercettato più volte Abu Musab al-Zarkawi, sospettato di appartenere ad Al Qaida, mentre ordinava attacchi terroristici contro obiettivi ebraici in Germania. Le intercettazioni hanno portato a individuare e distruggere una cellula terroristica ma non ancora a fermare al-Zarkawi, che pare ora si affidi a telefonate brevissime, ognuna di poche parole in codice.

Computer a rischio e nessuno ce lo ha detto! Quando Microsoft scopre i bug dentro Windows può aspettare anche sei mesi a dirlo.

E intanto il problema è nostro...

L'ULTIMA FREGATURA MICROSOFT
il Bug dei Duecento Giorni

Diciamo che la serratura di casa nostra è rotta e basta girare la maniglia per entrare. Diciamo che aspettiamo sei mesi prima di metterla a posto, nonostante in paese lo sappiano tutti. Diciamo che siamo distratti, o peggio? Come chiamare allora Microsoft, che fa la stessa cosa ma a spese nostre? Le serrature le fa lei, ma la casa in pericolo è la nostra. E non è roba da poco. In Gibson Research, esperta in sicurezza, ha chiamato il bug di cui parliamo la madre di tutte le vulnerabilità di Windows, dato che permette a un aggressore di assumere il controllo totale di un computer Windows remoto in vari modi, neanche così improbabili.Chi usa Outlook e Outlook Express spalancano letteralmente la porta all'attacco, così come le macchine Windows con network binding di default e non protetti da un router NAT o da un firewall. Il tutto su Windows 2000, NT, XP e 2003.

La buona notizia: Microsoft ha rilasciato una patch che sistema il problema. Ma, come detto, arriva più di sei mesi dopo che il problema è stato scoperto.
Nel frattempo chissà quante macchine sono state compromesse, da qualche furbone che sapeva già tutto o lo ha scoperto cammin facendo... Ecco dove siamo vulnerabili senza patch.

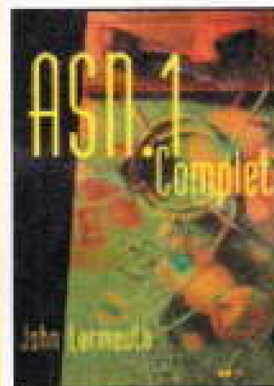
> *Il bug è stato scoperto il 18 agosto. Microsoft lo ha lasciato aperto fino al 10 febbraio: 186 giorni*

Il bug è il numero 828028, descritto da Microsoft nel suo bollettino di sicurezza MS04-007, emesso il 10 febbraio 2004 (il bug è stato scoperto il 18 agosto 2003, fonte http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0818). Il bollettino si può leggere per esteso all'indirizzo http://www.microsoft. com/technet/ security/bulletin/MS04-007.mspx; noi ne riportiamo le parti essenziali e, naturalmente, rendiamo in italiano la spiegazione inglese originale.

È una vulnerabilità definita critica e si raccomanda che gli amministratori di sistema installino la patch appena possono. Il file vulnerabile si chia-

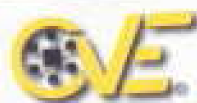
TUTTO SU ASN.1

Per scoprire come funziona ASN.1 e, se possibile, qualche altro bug, niente di meglio che i libri liberamente scaricabili a http://www.oss.com/asn1/booksintro.html.



ASN.1, un sistema complesso di strutturazione dei dati per l'uso tra più applicazioni, che in Microsoft non sono stati tanto capaci di fare funzionare come si deve





Common Vulnerabilities and Exposures

ma Msasn1.dll; se è presente nel sistema, la patch deve essere installata. Gli aggiornamenti automatici di Windows si accorgono del problema e quindi scaricano la patch da soli... ammesso che l'aggiornamento sia attivato.

Su una installazione base di Windows XP [illegible], ma viene installato dall'aggiornamento per la sicurezza (!) descritto all'indirizzo http://www.microsoft.com/technet/security/bulletin/ms03-041.mspx Il bug affligge la libreria ASN.1. L'acronimo sta per Abstract Syntax Notation e riguarda uno standard di dati usato per la normalizzazione degli stessi da una piattaforma all'altra. Maggiori informazioni su ASN.1 sono disponibili all'indirizzo http://support.microsoft.com/default.aspx? scid=kb;en-%20us;252648. Il rischio maggiore si verifica se l'aggressore è all'interno della rete in cui sta la vittima ma, per quanto meno probabile, il rischio è presente anche se questa condizione non è verificata.



▲ *A volte i bachi nel software sono grossi e visibili, ma restano lì per centinaia si giorni, soprattutto in casa Microsoft.*

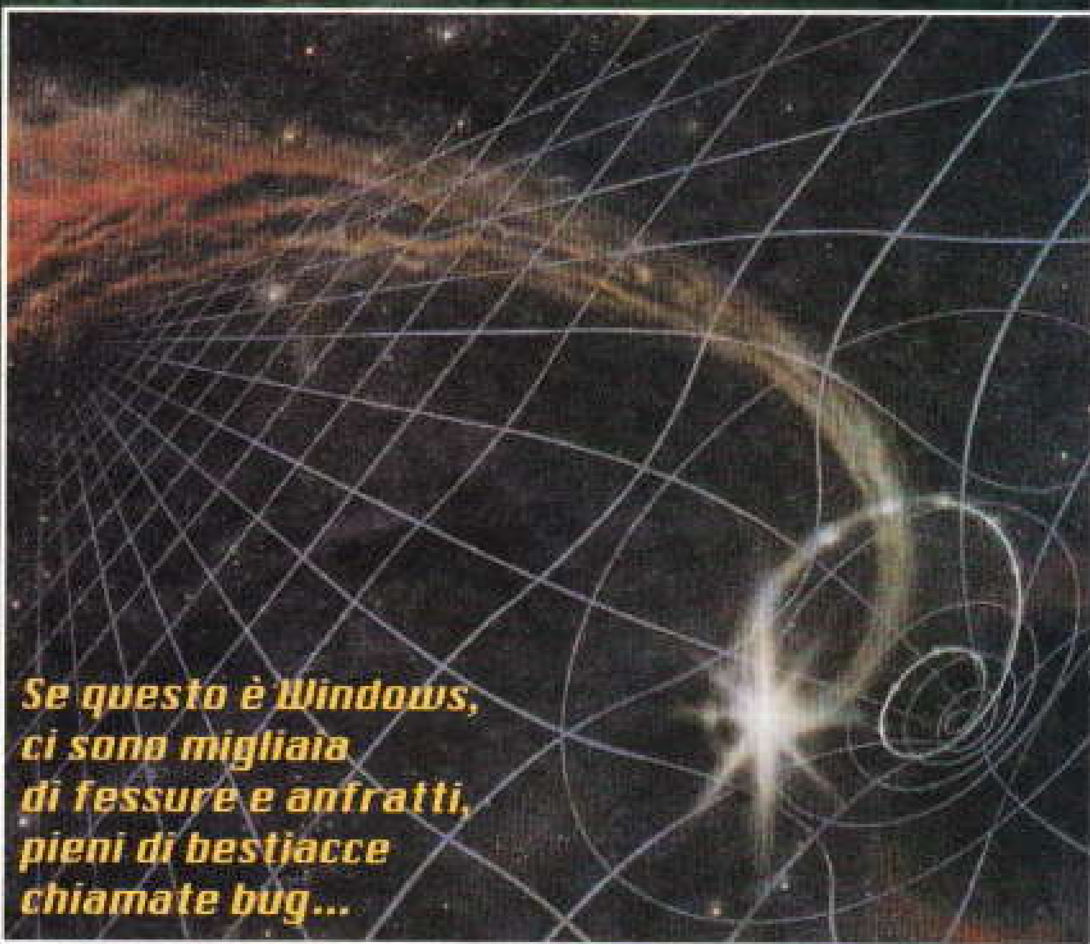
L'attacco possibile è un buffer overrun, causato da un tentativo riuscito di forzare il computer (più facilmente un server) a decodificare codice ASN.1 malefico, per esempio durante l'uso di un protocollo di autenticazione basato su ASN.1. L'aggressore può assumere il controllo totale della macchina e fare qualsiasi cosa, compreso installare programmi, guardarsi tutti i dati, modificare o cancellare quello che vuole e, naturalmente, creare nuovi account utente dotati di tutti i privilegi possibili. Tutto questo è possibile perché la libreria ha un buffer difettoso.

La lezione non servirà

Finita qui? Per niente. Dando un'occhiata alla pagina http://www.eeye.com/html/Research/Upcoming/index.html ci si accorge che altri ricercatori di sicurezza, appunto a eEye, hanno identificato oltre sette mesi fa (esattamente il 10 settembre e l'8 ottobre) altre tre vulnerabilità che permettono di eseguire codice su una macchina remota e prenderne il controllo. Il mondo lo sa, Microsoft aspetta, e intanto? Siamo a rischio...

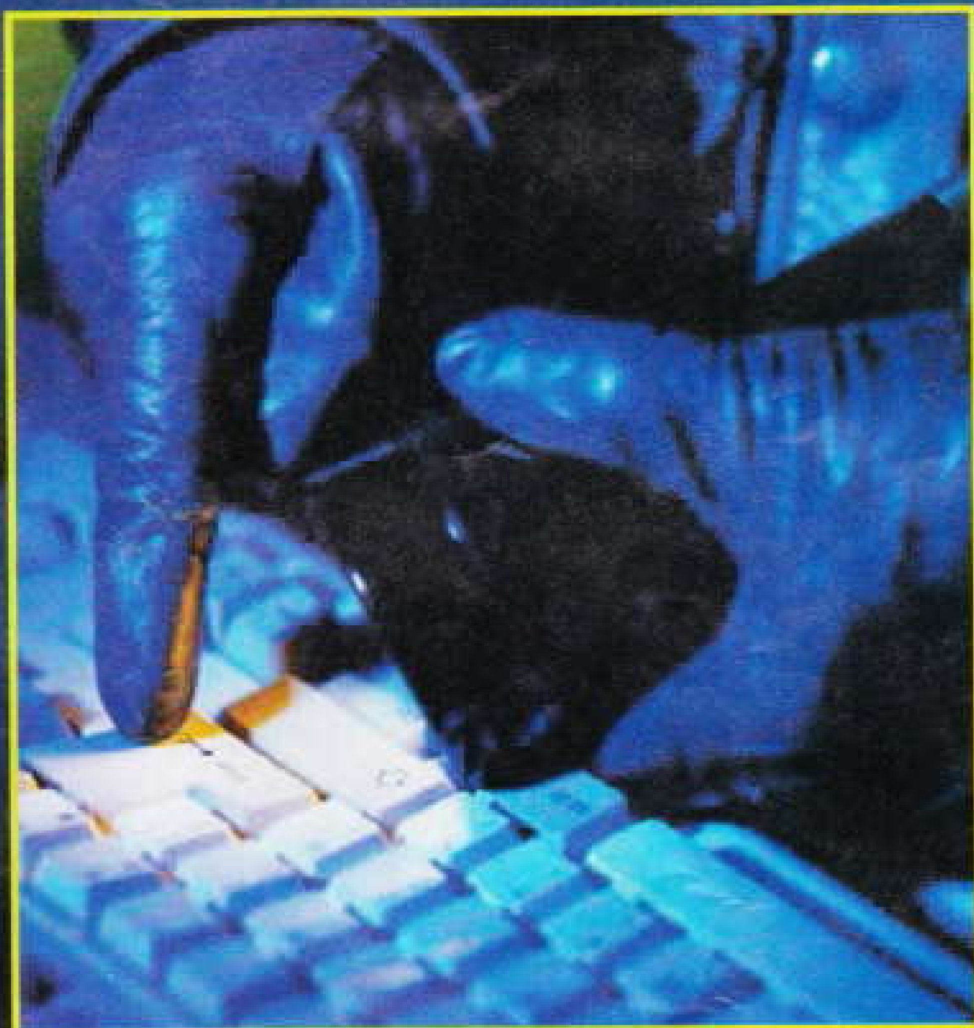
Michele Campovecchio
michele_c@hackerjournal.it





NON TOCCARE

La stanza è indifesa, qualcuno ha usato il nostro computer. Ecco come fare a tenere tutto sotto controllo



Un keylogger è un sistema che registra tutto quello che battiamo sulla tastiera del nostro computer e, a volte, anche qualcosa in più. In pratica ogni volta che pigiamo un tasto, il corrispondente carattere è memorizzato in un file che spesso possiamo leggere subito anche da remoto, oppure possiamo analizzare con calma più avanti nel tempo.

Perché utilizzare un keylogger?

Le possibilità di uso sono molte, ma quelle che vogliamo suggerire sono legate alla sicurezza del nostro computer.



◄ *KeyGhost Pro SE permette di memorizzare più di 2MB di caratteri crittati ed è classificato anche come materiale non esportabile nei 'paesi nemici' secondo la codifica militare della NATO.*

Potendo registrare tutto quello che è avvenuto, dai siti chiesti alle password digitate, abbiamo sempre la possibilità di:

QUEL TASTO!

- **controllare** che altri non abbiano usato il nostro pc;
- **verificare,** se l'abbiamo dato in uso ad altre persone, che non l'abbiano usato per scopi illeciti o indesiderati;
- **recuperare password** perdute o dimenticate, che magari abbiamo utilizzato solo una volta in una determinata occasione;
- **recuperare le ricerche** effettuate su rete di cui abbiamo perso traccia, ma che ancora ci servirebbero;
- **ricordare** cosa avevamo detto in una sessione di chat con una ragazza che risultava particolarmente simpatica;
- **recuperare la stringa PGP** che aveva criptato un messaggio: ci vorrebbero altrimenti anni di elaborazione per cercare di recupare il messaggio senza la corretta sequenza...
- **e chissà quante altre cose ancora!**

Se poi lavoriamo in qualche ufficio o abbiamo amici che lavorano, installare un keylogger sui pc in uso può esserci d'aiuto per tenere traccia degli utilizzi non autorizzati delle attrezzature aziendali, anche se in tal caso dovremo stare bene attenti a rispettare le regole di privacy e di politica aziendale.

Un esempio

Ecco cosa potrebbe dirci un file di log di un keylogger:

```
<PWR><ctrl-alt-del>Administrator<tab>carpet85<ent><ent>www.google.com<ent><ent>badbarbie<ent>

<PWR><ctrl-alt-del>Enrico<tab>sanna23<ent><lft><lft><pgu><ent>giovanni68@softhome.com<ent>Avrei bisogno che mi mettessi sul sito FTP i file che ti ho chiesto. La password per entrarci ti ricordo che è swinger45 (spero che non mi abbiano installato un keylogger!).
```

(prosegue a p 14)...



Montare un keylogger hardware? Semplicissimo: si stacca il cavo della tastiera, si inserisce il keylogger e si riattacca

I LINK UTILI

http://www.amecisco.com/iks2k21d.exe
una demo scaricabile di un keylogger software



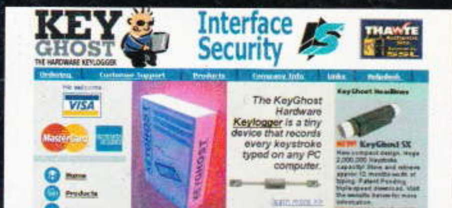
http://www.kmint21.com/keylogger/keylogger.zip
la versione free di un keylogger software



http://www.refog.com/
keyboard spectator, software in versione demo



http://www.keyghost.com/sx/
la versione più semplice da installare di un keylogger hardware



...(prosegue da p 13)

<ent>enrico86@hotmail.com<ent>Ciao, questo devi vederlo, ma possibilmente non quando c'è davanti al video la tua fidanzata... ;) http://www.bikini.com

<PWR><ctrl-alt-del>Ciccio<tab>agosto15<ent><ent>www.hotmail.com <ent>Ciccio9812<tab>trippa23<ent> http://www.l0pht.com/<ent>



Come leggerlo

Dagli esempi vediamo subito un paio di cose: un keylogger registra tutto, sia i caratteri in chiaro, sia quelli di controllo. Così, ogni volta che accendiamo il computer, appare il codice <pwr>. Quando l'utente vuole accedere a un sistema NT, gli viene chiesto il login dopo aver premuto Ctrl+Alt+Del e qui vediamo in chiaro gli user ID e le password di ciascuno. L'amministratore di sistema, per esempio, ha la password carpet85. Niente male.

Il secondo utilizzatore, Enrico, ha spedito una email a giovanni68 dicendogli la password di un sito FTP su cui scaricare dei file. Il quarto è andato su una pagina che richiede l'identificazione dell'utente ed evidentemente era registrato come UserID: Ciccio9812 e pw:Trippa23

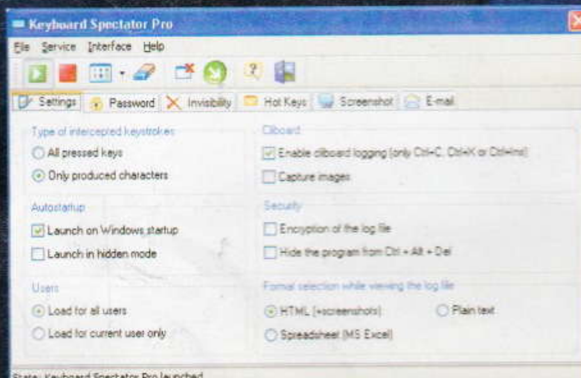
Software o hardware?

I keylogger possono essere software o hardware. L'invisibilità totale la si ottiene ovviamente tramite quelli software, ma quelli hardware hanno il vantaggio di non influire in nessun modo con la velocità della macchina, di non essere scopribili con i normali software scanner e quindi di passare inosservati, soprattutto se stiamo operando in un ambiente di persone non troppo esperte o attente agli accessori hardware del proprio PC. I keylogger software possono, a loro volta essere di due tipi:

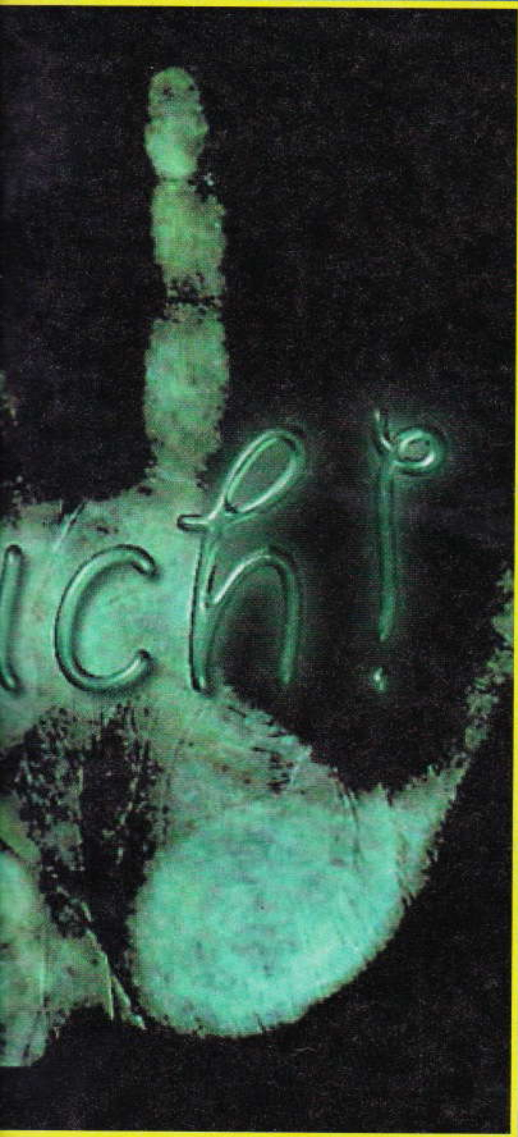
- visibili nel Task Manager, oppure
- totalmente invisibili

Ovviamente i primi si disabilitano facilmente, proprio usando Task Manager, mentre i secondi rimangono invisibili fino a che non utilizziamo un sw che li possa svelare, come spyhunter, spycop o quanti altri. Una cosa che accomuna tutti i keylogger software è comunque quella di registrare su disco il file dei caratteri catturati e quindi, da qualche parte, sono sempre intercettabili. I keylogger hardware si basano normalmente su un cavetto 'maggiorato' che si collega tra il cavo della tastira e la porta d'ingresso della tastiera stessa sul PC. A volte sono addirittura integrati nella stessa tastiera, che è stata ovviamente opportunamente modificata rispetto alla nostra tastiera usuale. In quest'ultimo caso sono, naturalmente, i più subdoli e i meno intercettabili, perché proprio non si vedono.

Il file, in questi casi, non è nemmeno registrato su disco, ma addirittura all'interno di una memoria flash nel dispositivo stesso. La capacità a cui

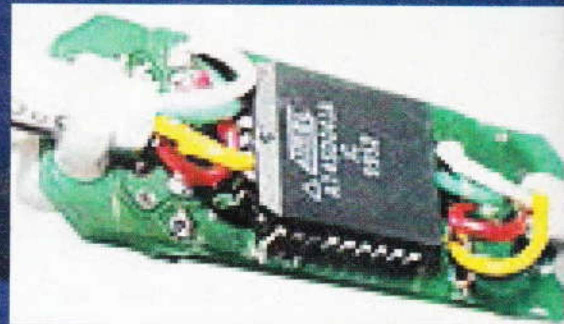


▲ *Una tipica finestra per usare al meglio un keylogger software, in questo caso Keyboard Spectator.*





◄ ▼ *All'interno di una tastiera appositamente modificata può essere installato un keylogger: non lo scopriremo mai.*



Come sceglierli

Di keylogger, in rete, ne troviamo a bizzeffe. Se ci facciamo un po' di domande e quindi leggiamo le caratteristiche, possiamo capire cosa realmente ci può servire per migliorare la sicurezza del nostro PC, rispetto agli utilizzi indesiderati. Eccone alcune possibili:

- **le informazioni** che saranno catturate hanno quasi sempre un grado di riservatezza elevato?
- **il computer** è connesso a Internet?
- **si collegano** al computer utenti differenti?
- **siamo interessati** alle informazioni sia in uscita che in entrata?
- **ci serve** che vengano catturate anche le schermate?
- **dev'essere un sistema** completamente invisibile?
- **il PC è utilizzato** da un utente esperto o da un newbie?
- **esiste** una porta USB?
- **il PC** è un desktop o un notebook?
- **viene spostato** spesso da un posto all'altro?
- **abbiamo l'accesso** come amministratori?
- **per quanto tempo** abbiamo intenzione di monitorare il PC?

Sulla base delle risposte che abbiamo dato a queste informazioni e usando un po' di fantasia, siamo così in grado di capire meglio quale sistema, software o hardware, è meglio che utilizziamo e di che tipo deve essere: cose come capienza della memoria e dimensioni, per esempio.

standardbus
standardbus@softhome.net

possono arrivare queste memorie è sufficiente, utilizzando appositi algoritmi di compressione integrati, per registrare circa un anno di attività del computer stesso. Per poi ricominciare automaticamente a ricoprire i dati a partire da quelli più vecchi.
Il microprocessore interno a questi dispositivi, che prende l'alimentazione dalla linea stessa che alimenta anche la tastiera, è in grado di crittare pesantemente i dati catturati, per cui è materialmente impossibile da parte di chiunque decifrare quanto registrato.
A meno, ovviamente, di essere gli spioni che l'hanno installato. Pensandoci bene, perfino se l'utente del computer decide di sostituire e distruggere il proprio hard disk, saremo in grado di avere tutti i suoi dati sensibili intatti, purché li abbia battuti sulla tastiera almeno una volta all'anno.



COME SI RECUPERANO I DATI

In un keylogger hardware è sufficiente battere sulla tastiera, dentro qualunque editor di testo e in qualunque momento:

la-mia-password-del-keylogger

Naturalmente dovrà essere una password sufficientemente difficile da scrivere per pura combinazione...

Appare un menu analogo a questo, da cui scegliere l'azione che si desidera:

Menu >

❶ Entire log download [get entire log]

❷ Section log download [get part of log]

❸ Erase log [erase log quickly]
❹ Format [securely wipe log (slower)]

❺ Options [filter or record arrow keys]

❻ Optimize speed [increase the retrieval speed]

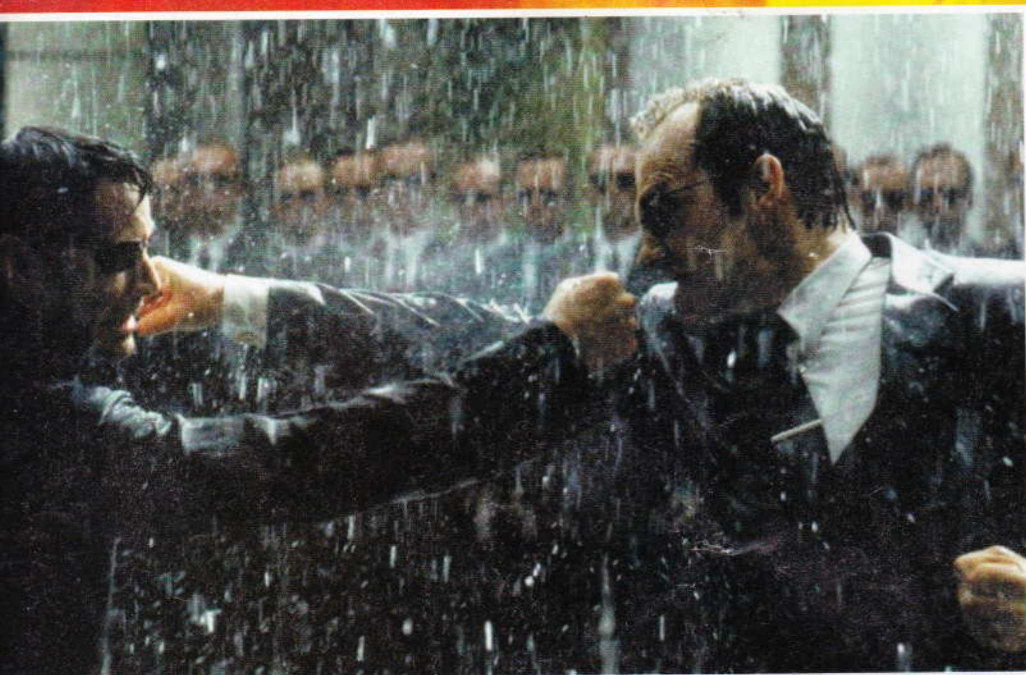
❼ Password change [change PUC password]

❽ eXit [exit the access menu]

Select > _



Alla PALLIDA LUCE

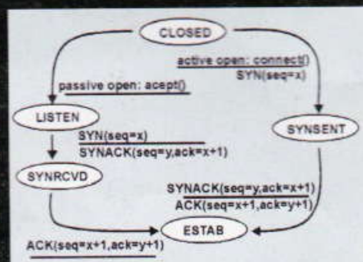


Stava attento a ogni particolare, ma quella sera maledetta sarebbe stata solo l'inizio. Verges si scontrò con un suo degno avversario: un consulente per la sicurezza della coldless.com

S'attaccò alla prima chat che gli venne tra i piedi in mezzo al browser. Gli sembrava di essere ai tempi dei CB, i citizen band sempre pronti a lanciarsi in discussioni sugli argomenti più futili, per lo più sempre interrotti da qualcuno che dire che stava usando delle parole volgari era come dargli del principino. Li capiva, dovevano essere usciti da qualche serata così.

Ne scelse uno a caso, di nick: Catrace, e si buttò nella mischia.
L'occasione gli venne offerta da Verges, che ingenuamente chiese se qualcuno potesse aiutarlo a scrivere un driver in C++ per un progettino che stava pensando di costruirsi a casa sua.
wFu la gentilezza con cui formulò la domanda? Gli psicologi di quella che viene gentilmente definita una "casa circondariale", null'altro che un luridissimo carcere in Texas, successivamente al suo arresto, lo aiutarono a capire che in realtà era un senso di frustrazione mai chiaramente emerso, derivante da chissà quale esperienza, sicuramente esaltato dai suoi insuccessi con le ragazze, dalla sua misantropia e da un mucchio di altre cazzate che misero in forse perfino l'educazione della nonna di sua nonna. Un fattore genetico, quasi. Ma con ordine, tutto iniziò per un innocuo finger e terminò per un telnet di troppo.

All'ingenua domanda di Verges, Catrace rispose con un RTFM, read the f*ing manual.**
Chiunque altro si sarebbe immediatamente lanciato in una risposta altrettanto vigliacca e deludente, scatenando un flame: lo sfogo e lo scopo di Catrace. Ma non Verges. Si limitò a rispondergli "Newbie!" e lo lasciò alla derisione degli altri. È per vendetta, quindi, che Catrace iniziò tutti i suoi guai.
Usò un comando finger sull'IRC a cui si era collegato e acchiappò al volo l'email di quel cretino: verges@coldless.com. Gli venne come un'intuizione, che successivamente pagò ben più cara del previsto, ma confermò l'intuito che gli veniva riconosciuto. Un telnet al server di posta della coldless.com con un bel "expn root@coldless.com" gli diede la conferma: verges era nientepopodimenoché l'amministratore del sistema!



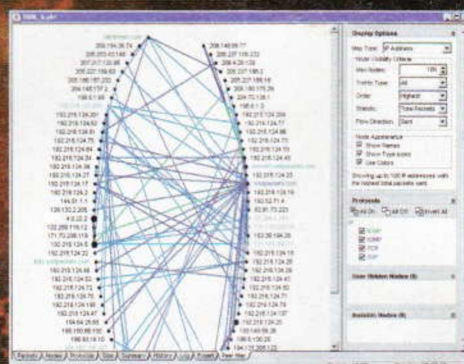
Salivava più del necessario, ma ormai la sfida era aperta. Gli avrebbe fatto pagare quel "newbie" pronunciato così a scherno, senza nemmeno conoscerlo. Aveva da poco scaricato Strobe, un programmino trovato su chissà quale sito underground. Uno scanner, che lanciò subito sul dominio coldless.com. Le porte gli sarebbero state elencate con meticolosità certosina e dovizia di particolari. Tutte potenziali punti d'ingresso o perché aperte o perché, probabilmente,

del monitor

attaccabili tramite qualche falla di sistema. Ma Strobe sbatté sul firewall. Il quale confrontò in due microsecondi i pacchetti dei dati inviati da Catrace e la porta a cui erano indirizzati e decretò, nel microsecondo successivo, che cozzavano con le regole imposte dal suo amministratore di sistema. Un task di sistema rispose all'indirizzo del PC di Catrace con una stringa di caratteri random che saturarono la connessione e nel frattempo un'email avvertiva l'ISP di Catrace, con messaggio standard, che l'account era stato usato con uno scanner di porte. Il server dell'ISP chiuse l'account in circa due minuti per sospetta illegalità e registrò l'evento nel file di log che l'amministratore avrebbe letto il mattino successivo. Catrace si trovò senza connessione di botto, ma poco importava: era una di quelle a costo zero recuperate dal primo ISP pubblico che gli era capitato sottomano, registrandosi con nomi e indirizzi totalmente fittizi. Proprio quella che utilizzava normalmente per sondare i terreni inesplorati.

Scansò il momentaneo inconveniente ricollegandosi a un altro provider free, sapendo bene che senza ripetizione dell'evento nemmeno l'ISP avrebbe approfondito più di tanto: tempo e soldi sprecati per qualcuno che aveva fatto solamente una prova, tra i mille e passa di quella stessa notte. Dalla cassetta degli attrezzi, si fa per dire, recuperò un software che gli era parso sufficientemente intelligente: uno stealth port scanner, il cui punto di forza – che lo rendeva invisibile, o quasi - era quello di spedire un pacchetto FIN, con settato a uno il flag di FINe della trasmissione, in un momento sbagliato. Ovvero prematuramente (vedi "SYN, ACK e FIN: come t'imbroglio la trasmissione"). Quello che Catrace non aveva previsto è che le informazioni inviate nel pacchetto dello stealth port scanner da lui scelto erano comunque sufficienti per identificarne la provenienza.
La risposta dello scanner diede due informazioni a Catrace: il server della coldless.com era utilizzato per transazioni sicure e criptate e per i servizi Web. Ma una cosa fece sussultare Catrace: sembrava proprio che una porta assurda, la 31654, fosse stata messa lì apposta per essere aperta e disponibile all'ingresso nel sistema. Qualcun altro prima di lui aveva già tentato e s'era preparato una back door, un passaggio segreto pronto per la successiva e più profonda incursione?

Un programmino di chiamata automatica al cellulare di Verges lo svegliò con un SMS d'allarme intrusione. Due minuti dopo era attaccato al terminale e stava entrando nel sistema a lui affidato: in fondo i lunghi studi universitari dopo la praticaccia della passione, che lo aveva spinto a diventare un consulente per la sicurezza, venivano utili proprio in questi momenti. C'era da capire perché EtherPeek, lo sniffer che aveva da poco installato sul sistema, si era deciso proprio adesso a svegliarlo alle luci dell'alba. Ma non trovò nulla. Nessuna attività, niente di niente. Catrace s'era appena scollegato: l'intuizione, ancora. Aveva deciso che sarebbe stata una decisione salutare rimandare l'approfondimento alla notte successiva. Curioso com'era, anche Verges non si diede per vinto. Il mattino successivo, al ritorno in ufficio, scandagliò ogni riga del log di sistema. E lo beccò. Una telefonata all'ISP e anche il secondo account di Catrace venne chiuso, ma nella risposta negarono a Doberry ogni altra indagine approfondita sulle generalità dell'account: sarebbe stata una violazione alla privacy, che non era nella politica adottata da quello specifico ISP. Ancora una volta un punto per Catrace.



La schermata di EtherPeek che Verges amava di più

Ma in realtà, senza saperlo, aveva solo prolungato la sua agonia…

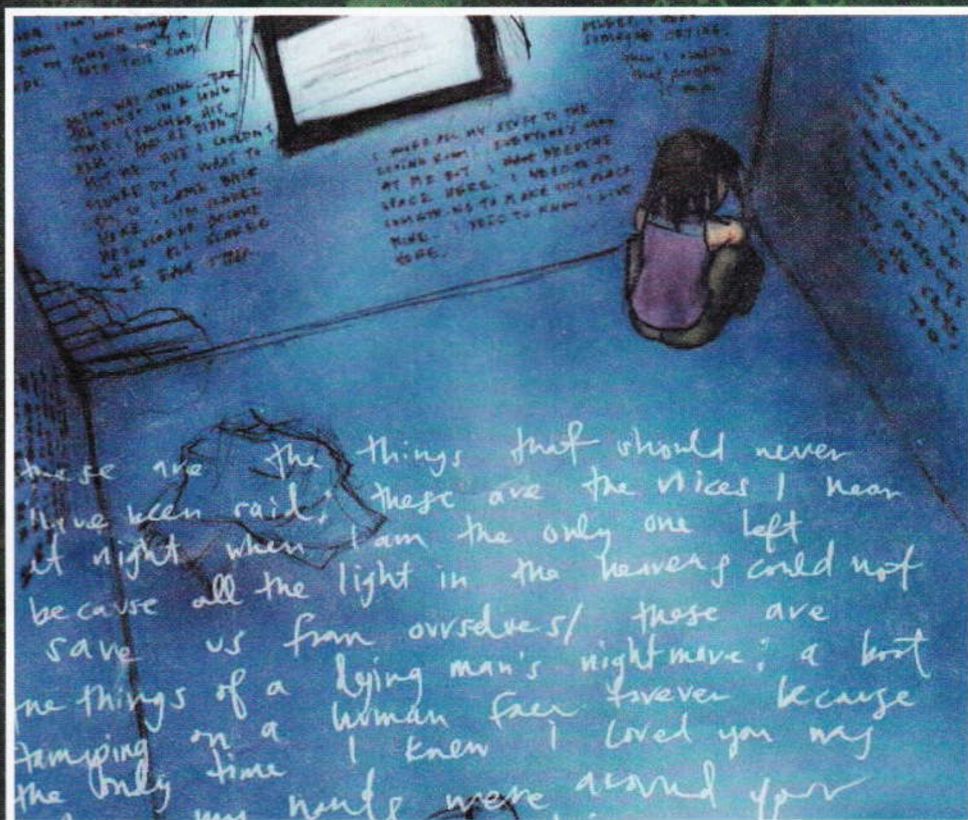
WriterBus

…SEI SETTIMANE DOPO

Di notte in notte, di prova in prova. Catrace diede fondo alla sua esperienza di smanettone delle profondità della rete. Non era più rabbia, ma sfida. Non era più vendetta, ma droga. Un sottile compiacimento per la sua bravura lo teneva legato a 'quella' pallida luce del monitor, di ora in ora, di notte in notte…
A Verges non pensava quasi più, era sprofondato nella caccia a tutto quello che si muoveva, dentro quel server coldless.com. E non tenne più conto della paura. Usò direttamente telnet sull'ormai svelato database dei numeri di carte di credito del sistema di e-commerce, quello a cui Verges, nemmeno a dirlo, teneva di più.Era allo scoperto, ma non se ne rese conto. Verges invece sì.
Alla sentenza teneva ancora in mano il CD contenente il log di sistema e la copia del file scaricato dall'utente specificato in alto a sinistra, voce 'IP address'. L'aveva evidenziato in grassetto, per farlo notare meglio al giudice: una femmina di colore in una grintosa e paludata acconciatura. Mentre l'FBI portava in aula altro materiale sequestrato, nonché Catrace in persona: cui furono rimesse le manette, quando venne il momento di passare dall'aula di tribunale al carcere. Tre anni, senza condizionale.

SEMPLIFICHIAMOCI

Possiamo fare sostituzioni incredibili nei nostri testi grazie alle espressioni regolari, o regex



CHI HA RISPOSTO SULLE DATE

Un grosso grazie a Jerk, Nixxo, Buffer Overflow e DarkLink per avere risposto ai quesiti degli scorsi articoli. DarkLink poneva varie osservazioni di impostazione, tutte corrette. Nixxo individuava correttamente giorno mese e anno, con qualche limitazione di cui era consapevole. Bravo. Jerk ha sviluppato una espressione regolare che dovrebbe risolvere il problema delle date al 99 percento, con una sola eccezione: il 29 febbraio (quest'anno ce n'è stato uno). La sua regex è (([0-9][0-9][0-9][0-9][/-._;](1|[3-9])|(0(1|[3-9])|1[012])[/-._;][1-9]|([012][1-9]|3[01]))|([1-9]|([012][1-9]|3[01])[/-._;](1|[3-9])|(0(1|[3-9])|1[012])[/-._;][0-9][0-9][0-9][0-9]))|(([0-9][0-9][0-9][0-9][/-._;]2|02[/-._;][1-9]|([012][1-9]))|([1-9]|([012][1-9])[/-._;]2|02[/-._;][0-9][0-9][0-9][0-9]))

Veramente un gran lavoro!
Chi sa dire se è corretta? Qualcuno sa elaborare una regex definitiva, che trovi giorno mese e anno in tutti i modi possibili, senza fare errori?

Nell'ultimo articolo sulle regex avevamo chiuso con due domande: ❶ catturare gli indirizzi di posta all'interno di un testo; ❷ dato un file contenente il testo

Andy Serkis
Billy Boyd
Cate Blanchett
Christopher Lee
Dominic Monaghan
Elijah Wood
Hugo Weaving
Ian Holm
Ian McKellen
Liv Tyler
Sean Astin
Viggo Mortensen

con un programma che consente di fare ricerca e sostituzione con le espressioni regolari, cerchiamo ([a-zA-Z]+)( )([a-zA-Z]+) e lo sostituiamo con \3\2\1. Che succede al file? Soprattutto, perché?

La risposta migliore l'ha data Daniele Midi

Salve,
mi chiamo Daniele ed ho 15 anni. Ormai da parecchi anni mi diletto nella programmazione Windows, e posso dire anche di essere piuttosto bravo. [...] volevo proporre le soluzioni dell'ultimo quesito da voi posto sempre sulle Regex:

[a-zA-Z.:-]@[a-zA-Z.:-]*.[a-zA-Z]**

per quanto riguarda gli indirizzi e-mail e...

la vita con le REGEX

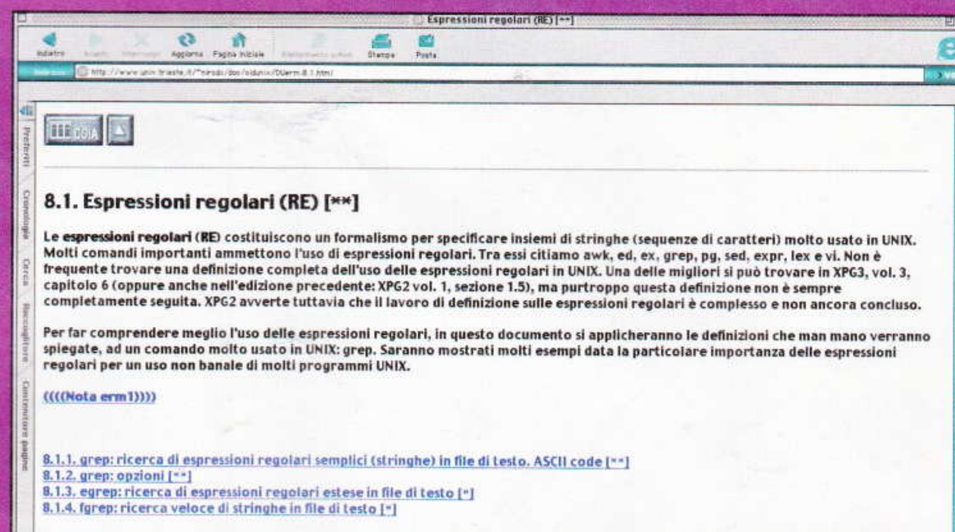
CONOSCERE I DIALETTI

Le espressioni regolari che pubblichiamo sono il più possibile semplici e adatte a tutti i sistemi. È possibile tuttavia che in alcune situazioni (per esempio nella programmazione Java) la sintassi sia leggermente diversa. In generale tutte le nostre regex sono compatibili Perl. Per gli altri sistemi può essere necessario modificare qualcosa.



SITI REGOLARI

Su questi siti si può imparare molto in fatto di regex:
http://it.diveintopython.org/dialect_re.html (in italiano)
http://www.biocomp.unibo.it/piero/corso/note/node69.html (in italiano)
http://www.corsolinux.it/testi/perl/analog/le_espressioni_regolari.jsp (in italiano)
http://www.english.uga.edu/humcomp/perl/regex2a.html
http://www.html.it/perl/perl_11.htm (in italiano)
http://www.lc.yi.org/scribble/scribble_show.php3?sid=226
http://www.regenechsen.de/regex_en/regex_1_en.html
http://www.regular-expressions.info/
http://www.silverstones.com/thebat/Regex.html
http://www.univ.trieste.it/~nircdc/doc/oldunix/DUerm.8.1.html (in italiano)



8.1. Espressioni regolari (RE) [**]

Le **espressioni regolari** (RE) costituiscono un formalismo per specificare insiemi di stringhe (sequenze di caratteri) molto usato in UNIX. Molti comandi importanti ammettono l'uso di espressioni regolari. Tra essi citiamo awk, ed, ex, grep, pg, sed, expr, lex e vi. Non è frequente trovare una definizione completa dell'uso delle espressioni regolari in UNIX. Una delle migliori si può trovare in XPG3, vol. 3, capitolo 6 (oppure anche nell'edizione precedente: XPG2 vol. 1, sezione 1.5), ma purtroppo questa definizione non è sempre completamente seguita. XPG2 avverte tuttavia che il lavoro di definizione sulle espressioni regolari è complesso e non ancora concluso.

Per far comprendere meglio l'uso delle espressioni regolari, in questo documento si applicheranno le definizioni che man mano verranno spiegate, ad un comando molto usato in UNIX: grep. Saranno mostrati molti esempi data la particolare importanza delle espressioni regolari per un uso non banale di molti programmi UNIX.

((((Nota erm1))))

8.1.1. grep: ricerca di espressioni regolari semplici (stringhe) in file di testo. ASCII code [**]
8.1.2. grep: opzioni [**]
8.1.3. egrep: ricerca di espressioni regolari estese in file di testo [*]
8.1.4. fgrep: ricerca veloce di stringhe in file di testo [*]

Bravo Daniele, ma si può fare meglio. I caratteri ammessi da un indirizzo di posta sono più di quelli che includi tu; per esempio possiamo avere underscore (_). Secondariamente, a destra della chiocciola possono esserci più di due gruppi di caratteri separati dal punto: per esempio, mario_rossi@mail.inet.it è un indirizzo corretto e a destra di @ ci sono tre sequenze di caratteri separate dal punto.
Come scrivere, allora una regex che legge correttamente un indirizzo di posta elettronica?

Ridiamo la parola a Daniele

Circa la seconda domanda su cosa facesse l'algoritmo di ricerca e sostituzione ([a-zA-Z]+)( )([a-zA-Z]+) sostituito con \3\2\1 in un elenco di nomi e cognomi, scambia i nomi con i cognomi.

Giusto! Nelle regex il parametro \1 sta per il contenuto della prima parentesi tonda. \2 si riferisce al contenuto della seconda parentesi tonda e così via.

Questi però erano nomi semplici, nel formato nome-cognome.
Come possiamo fare per questi?

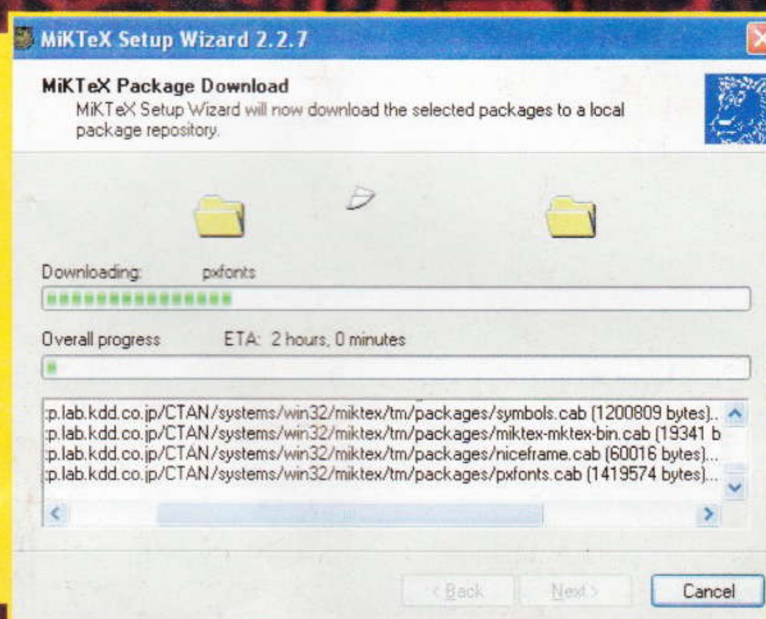
John Rhys-Davies
Sinead O'Connor
Christian De Sica

Per i primi due è solo questione di aggiungere il carattere giusto al riconoscimento. E il terzo, in che modo lo riconosciamo?

Barg the Gnoll
gnoll@hackerjournal.it

PORTIAMO LYX

NE ABBIAMO PARLATO, MA LE RICHIESTE ARRIVANO A FROTTE: È POSSIBILE INSTALLARE LYX SOTTO WINDOWS? DOBBIAMO, PRIMA DI TUTTO, PREPARARGLI L'AMBIENTE GIUSTO. ECCO COME

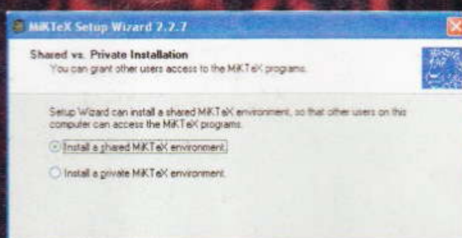


▲ *Un momento del download di MiKTeX*

LyX: ne abbiamo parlato sul numero 45 di Hacker Journal. Uno strumento che straccia Word e i suoi compari, in quanto a capacità di scrittura. Un elaboratore di testi che fa quello che desideriamo con intelligenza, e non fa quello che vuole lui. Un software in evoluzione perché Open Source.
Ora non rimane che installarlo e lo vogliamo fare sotto Windows.

Un sistema Unix, sotto Windows

LyX è nato sotto Unix e lì continua a vivere. Però, come tutti i progetti Open Source, il contributo di tante persone sparse per il mondo fa miracoli che sembrano impossibili: in modo del tutto gratuito, è possibile creare un ambiente che



▲ *Installando MiKTeX scegliamo, tendenzialmente, le opzioni di default*

lo possa accogliere e far funzionare nel modo migliore. Ecco cosa ci serve.

LaTeX

Per usare LyX serve LaTeX(2e), il potente motore che lo fa funzionare. Una distribuzione semplice di LaTeX è MiKTeX, che troviamo a http://www.mik-

È UTILE IMAGEMAGIK

ImageMagik è un programma che permette la conversione dei formati immagine in quasi tutti i modi attualmente conosciuti, ed è un programma free disponibile per quasi tutte le piattaforme. Serve a rendere disponibili le immagini nei formati riconoscibili da LyX.
Lo possiamo scaricare e installare da http://www.imagemagick.com/



DENTRO WINDOWS

tex.org/ nell'attuale versione 2.4.
Una molto più pesante da scaricare, ma completa di tutta una serie di funzionalità che altrimenti dovremmo recuperare successivamente, è fpTeX all'indirizzo http://www.fptex.org/. Purtroppo pesa circa 260 MB che vanno scaricati tutti. Scegliamo in base alla connessione internet che possediamo.
Ecco i principali passi che dobbiamo fare, nel primo caso:

1) scarichiamo MiKTeX 2.4 e poi seguiamo il Setup Wizard lanciando setup.exe; scegliamo Download Only e la versione Large per scaricare anche i font che servono a Windows. Dobbiamo anche cliccare su un sito geograficamente vicino, da cui scaricare il tutto. Dedichiamo una cartellina al software scaricato: per esempio creando C:\Temp\LyX\.
2) installiamolo lanciando di nuovo Setup.exe, scegliamo l'opzione Install Only sempre con l'opzione Large; seguiamo le opzioni di default;
3) cancelliamo i file di setup, ormai inutili.

Se abbiamo dubbi o vogliamo una guida ancor più dettagliata, andiamo sul sito http://www.miktex.org/ e seguiamo le indicazioni nelle apposite FAQ di installazione.

Installare LyX

Finalmente possiamo installare Lyx. Bisogna avere un po' di spirito da pionieri e un po' di esperienza. Consigliamo di consultare anche qualche sito di riferimento, utile per ogni eventualità, come per esempio http://www.chez.com/deuns/latex/lyx.htm, anche se le versioni variano velocemente e spesso sono state apportate migliorie che rendono obsoleto qualche passaggio.
Scarichiamo il software da http://www.home.zonnet.nl/rareitsma/lyx/lyx-1.3.3-win32.exe,

Download:

- lyx-1.3.3-win32.exe
- lyx-1.3.3-win32.r00
- lyx-1.3.3-win32.r01

For localized (native language) menus:

- lyx_intl.rar (eg for german set the following environment variable: LANG=de_DE)

▲ ***Per installare LyX dobbiamo scaricare tutti e tre i file nella stessa cartellina.***

normalmente in tre parti: un file .ex, un .r00 e un .r01. Scarichiamoli tutti e tre in un'unica cartellina.
Rinominiamo .ex in .exe e lanciamolo. Avviamo così l'installazione in C:\Programmi\LyX\. Terminata l'installazione cancelliamo i file ormai inutili, usati per l'installazione.

Eccoci pronti!

Quando avviamo il programma LyX.exe possiamo aprire uno dei file di esempio che si trovano in C:\Programmi\lyx\share\lyx\examples\. Questo corrisponde visivamente a una pagina web che varia con le dimensioni della finestra. Il risultato stampabile lo si può vedere premendo CTRL+D. Il risultato appare in una finestra dopo qualche momento d'attesa dovuto alla compilazione della pagina.
TeX lavora su un concetto di ambiente, quasi come parlassimo di "stili" di Word, con una scelta da una lista in alto a sinistra. L'ambiente Standard corrisponde al testo normale, Enumerate a una lista numerata automaticamente, mentre Itemize a una lista non numerata, e così via. I caratteri cambiano con il menu Layout | Character, e ci sono delle scorciatoie da tastiera: CTRL+B per il grassetto, CTRL+E per il corsivo e così via.

PREREQUISITI PER MIKTEX

MiKTeX Setup Wizard non installa nessun componente di sistema (cose come comctl32.dll). Prende per buono che sia già tutto installato alla versione più aggiornata. Quindi gli sono assolutamente necessari:

comctl32.dll
dobbiamo avere installata almeno la versione 5.80.2614.3600 della DLL Common Controls. Che è quanto avviene per XP o Me. Per sistemi più vecchi dobbiamo recuperare la DLL da Microsoft.

wininet.dll
dobbiamo avere installata almeno la versione 4.70.0.1300 di Internet Extensions DLL. Dovrebbe far parte di tutti gli Explorer dalla versione 4.0 in poi.

Se questi file non fossero installati, l'installazione s'interrompe con un messaggio di avvertimento.

STOP A WINDOWS E

È proprio vero che il sistema per gestire il nostro PC è così comodo e intuitivo? Se ci pensiamo bene no, ma possiamo recuperare dei validi rimedi



Abbiamo provato tutti ad avere sulla scrivania di Windows un po' di finestre aperte, anche solamente quattro o cinque. Già così siamo nei guai. Le possiamo sovrapporre, ma una nasconde l'altra e recuperare quella giusta è sempre un problema. Alt-Tab è l'ultimo dei rimedi, che comunque non ci toglie la scocciatura di non vedere il panorama completo di ciò che succede. La metafora della scrivania è stata abbastanza utile fino adesso, ma ora comincia a dare segni di cedimento.

Che senso ha avere disponibili un sacco di informazioni, se poi non le possiamo facilmente utilizzare? Meglio sarebbe avere un monitor grande quanto la scrivania vera su cui abbiamo appoggiato il computer, ma chi ci dice che dopo un po' anch'esso non si saturi? Siamo arrivati al punto di dover pensare diversamente l'interazione dell'uomo con il computer e gli studi, in tutti i laboratori del mondo, stanno portando a diverse soluzioni. Proviamo a esplorarne qualcuna.

Come si è cercato di rimediare

La prima a porre in atto un tentativo serio di soluzione è stata certamente Apple, con il suo Exposé (http://www.apple.com/macosx/features/expose/) di cui è dotato MacOS X. Con l'uso di tre tasti funzione è possibile disporre le finestre anche in modo di vederle tutte contemporaneamente e ben disposte sulla scrivania. Ed è certamente un bel passo in avanti. Microsoft, dal canto suo, propone MSVDM (http://www.microsoft.com/windowsxp/pro/downloads/powertoys.asp), il Virtual Desktop Manager che altro non fa che suddividere la scrivania in partizioni differenti di RAM, per cui da una videata suddivisa in quattro aree è possibile passare alle applicazioni aperte sull'una o sull'altra. Tutti modi di organizzazione dell'esistente, ma certamente non soluzioni radicali al problema.Ricordo un'utility inserita dal driver di un vecchio mouse (o era una scheda video) che attivava la finestra al passaggio del mouse. Carino, ma dopo 5 minuti veniva il mal di testa per il continuo cambiamento di finestra. Dopo la sbornia del "facciamo tutto con il mouse" sarebbe ora che i produttori riflettessero ancora un po' e cercassero una soluzione innovativa e veramente funzionale.

Alternative

Se passiamo a usare Unix, già le cose sono differenti, perché sono disponibili diversi window manager alternativi. Ma anche con Windows possiamo adottare altri metodi, per esempio scegliendo il progetto http://www.litestep.net/. Questo, come anche http://www.geoshell.com/index.asp, sono due shell alternative a Windows che trasformano radi-

ALLE SUE FINESTRE!

calmente l'organizzazione degli oggetti che troviamo sulla nostra scrivania virtuale. Ma non sono gli unici. Il concetto è quello del "tiling window manager", che divide gerarchicamente l'area di lavoro in pannelli orizzontali e verticali.

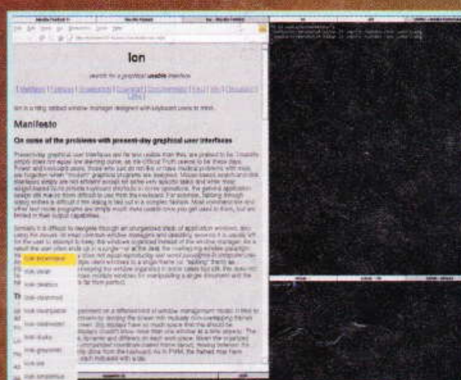
I vantaggi? Essenzialmente due:
- la parte attiva dello schermo è sempre ottimizzata al meglio, perché è dedicata a visualizzare la finestra in quel preciso momento attiva, senza altri elementi di sfondo o inutili rispetto a dove stiamo concentrando l'attenzione;
- ci diventa facile muoversi tra le finestre, perché così sono strutturate.

Non che manchino i problemi anche in un approccio del genere, perché nessuno di noi vorrebbe avere a pieno schermo, per esempio, una finestra di dialogo con scritto OK e Cancel, solo perché lì stiamo concentrando la nostra attenzione. Così diventa un problema per quelle applicazioni che aprono mille finestrelle di contorno, tutte facenti parte dell'attività in atto. Però la strada, a detta di molti, è proprio questa, e già che ci siamo ecco qualche indirizzo adatto a Windows, da cui possiamo scaricare delle interfacce di questo tipo:

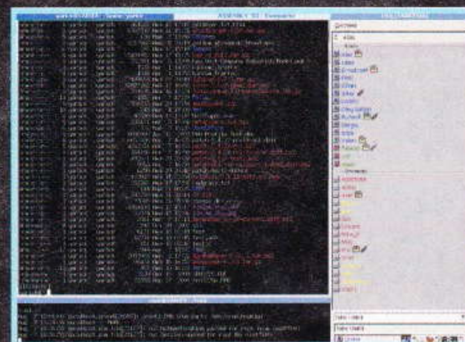
▲ Raptoison: http://ratpoison.sourceforge.net/; è il sistema più leggero e compatto, sulla falsariga di GNU Screen.



▲ FVWMPartition: http://www.imonk.com/baboon/FvwmPartition/ Piuttosto interessante perché prevede diverse finestre attive, pur in un ambiente suddiviso orizzontalmente e verticalmente.



▲ Ion: http://modeemi.cs.tut.fi/~tuomov/ion/ Oltre a sposare bene la filosofia del tiling window manager, gestisce diversi spazi virtuali, è scriptabile tramite Lua (un linguaggio Open Source).



▲ TrsWM: http://www.relex.ru/~yarick/trswm/; è basato sullo stesso motore di Ion, ma è un po' meno pulito. Segue la filosofia delle interfacce a suddivisione della scrivania, ma lascia spazio a una gestione più classica e quindi accetta qualche compromesso. Da provare in alternativa a Ion.

Sperimentare

Tutto ciò di cui abbiamo parlato è attualmente uno dei settori più vasti di ricerca, perché coinvolge l'interazione tra noi umani e le macchine che ci stanno intorno. Un campo in cui siamo solamente agli inizi, dopo i grandi successi delle interfacce così come le conosciamo oggi. Tutto sommato è passato parecchio tempo dal momento in cui Douglas Engelbart ha inventato il mouse allo XeroxPARC, ed è forse ora di pensare a qualche evoluzione altrettanto intelligente. Un ottimo soggetto per scatenare la fantasia di noi hacker.

One4Bus

Uccidiamo definitivamente Lo S

Ecco un sofisticatissimo sistema completamente gratuito che filtra tutto il testo indesiderato, da qualunque parte provenga. Potenza delle espressioni regolari



Si chiama CRM114 ed è un sistema, anzi un linguaggio vero e proprio, che ci permette di esaminare le e-mail in arrivo o anche i log di sistema, o qualunque altro insieme di dati, in modo da poterli organizzare, ordinare o filtrare secondo delle regole che abbiamo stabilito.

Ma il bello è che le regole non dobbiamo deciderle tutte in un colpo, ma possiamo farle imparare al filtro sulla base di esempi che via via gli diamo in pasto.

Per esempio possiamo impostare una regola di base che dica al sistema quali e-mail buttare sulla base di un pezzo di testo che le identifica come spam. Mano a mano che arrivano altre e-mail che sono spam e che non vengono riconosciute come tali, lo indichiamo al sistema il quale impara dagli errori e si comporta meglio la volta successiva.

DOVE CERCARE

Per avere tutte le informazioni necessarie sul 'come fare' e 'come funziona':
http://crm114.sourceforge.net/CRM114_Mailfilter_HOWTO.txt

Da leggere se vogliamo approfondire ogni aspetto della cosa:
http://crm114.sourceforge.net/FAQ.txt



◁ *Un logo decisamente carino. Scopriamo sul sito che è stato creato da Liz Manicatide, un bravo disegnatore che fa anche molte altre attività (http://www.emphasiscreative.com)*

L'autore del linguaggio assicura che dopo un giorno di allenamento intensivo e circa un mese di perfezionamenti, l'accuratezza supera il 99,9%, che significa che abbiamo trovato il filtro definitivo e preciso in grado di battere qualunque prodotto commerciale 'statico'.

Piuttosto complicato

Se definiamo CRM114 come un semplice filtro anti-spam, l'autore si arrabbia (e ha ragione). CRM114 è un vero e proprio linguaggio che rende possibile scrivere potenti filtri di ogni tipo e che possiamo fare agire su qualunque insieme di caratteri, anche particolarmente grande o complesso. La versione che scarichiamo liberamente dal sito http://crm114.sourceforge.net comprende degli esempi di filtri già scritti, per chi semplicemente vuole utilizzarlo, per esempio, come spam eliminator.

IMPARA DAGLI ERRORI

Per far capire meglio a CRM114 cosa è gradito e cosa no, dobbiamo adottare il sistema TOE: Train Only Errors. Cioè, tutte le volte che un'e-mail viene lasciata passare e quando invece è spam, bisogna dirglielo con l'apposita istruzione di comando. Ma non bisogna dirgli altro, perché altrimenti il metodo, invece che imparare, ci mette più tempo nel riconoscere la spazzatura.

Dopo qualche tempo, diciamo qualche giorno, l'accuratezza sale velocemente al 95% per stabilizzarsi in un periodo che va da quindici giorni a un mese su una percentuale di circa il 99,9%, meno di un errore su mille e-mail analizzate.



MA CHE NOME, DR STRANAMORE!

CRM114? E cosa vuole dire? Ufficialmente CRM sta per Controllable Regex Mutilator, ma la realtà è che nel film Dr Stranamore (in origine dr Strangelove) CRM114 è la macchina di decifrazione dei piani segreti della guerra fredda. La battuta originale in cui compare? Eccola:

GOLDIE: "Major Kong, I know you're gonna think this a crazy but I just got a message from base over the CRM 114. It decodes as Wing Attack plan R. R for Romeo" (tratto dal film dr Strangelove - Distribuzione Columbia Pictures, UK 1964)

Nel film, un generale dell'esercito americano concepisce un folle piano per mettere in moto il meccanismo sterminatore della guerra atomica, mentre i russi ne stanno approntando uno analogo denominato Fine del Mondo. Attivati i bombardieri atomici, non c'è speranza di richiamarli se non con la chiave cifrata incisa nella testa del matto che si è rinchiuso nella propria base militare. Il presidente degli Stati Uniti non può fare altro che avvertire il suo collega del Cremlino affinchè abbatta gli aggressori americani. Ma uno di essi sfugge alla distruzione...

E se non abbiamo visto il film, è obbligatorio trovare subito una copia VHS: è stato definito il migliore film satirico del secolo scorso!


William Yerazunis, il ricercatore dei laboratori MERL Mitsubishi e creatore di una montagna di progetti innovativi, tra i quali anche CRM114.

Il criterio utilizzato dal sistema si basa su difficili algoritmi statistici, basati su confronti binari polinomiali utilizzati coi criteri di Bayes e i modelli di Markov, modificati per migliorarne l'accuratezza. Lasciamo agli appassionati di statistica e matematica di approfondire l'argomento, che sul sito di CRM114 troviamo spiegato fino all'approfondimento che ciascuno può desiderare.

Si tratta di un'intelligente applicazione di espressioni regolari (RegEx) che migliorano con l'esperienza che il sistema acquisisce via via che gli diciamo quali errori sta commettendo. In altre parole, CRM114 è capace di imparare e lo fa anche velocemente.

Volendo, CRM114 è compatibile con i software che segnalano le e-mail considerate spam, come SpamAssassin.

Può anche essere usato come sistema di controllo dei log di sistema sui server o come filtro dei log generati dai firewall, per accorgersi subito delle intrusioni in atto o degli eventi strani o non usuali.

Dove funziona

CRM114 è uno strumento nato sotto Linux, ma come al solito, essendo un progetto OpenSource, è stato trasportato sotto altri sistemi tra i quali BSD, MacOSX, Windows NT sotto Cygwin ed è utilizzabile perfino con Outlook, sfruttandone le macro. Anche se il procedimento per farlo funzionare con Outlook è abbastanza complesso e richiede un po' di esperienza e un po' di spirito da sperimentatore, è descritto molto bene scaricando la documentazione e le macro dall'indirizzo http://www.signull.org/olcrm114.zip.

AGGIUNGERE LE LISTE NERE



Probabilmente tutte le e-mail che arrivano dal nostro boss devono essere lette comunque, anche se spesso le possiamo considerare spam della peggior specie...

Così anche le e-mail della nostra ex-ragazza: certo, sarebbero forse interessanti. Ma è altrettanto saggio buttarle immediatamente tutte nel cestino...

Ecco, sono due esempi di eccezioni che dovremmo impostare alle regole. Come fare? Semplice, si creano delle white-list o delle black-list.

Tutte si basano su apposite espressioni regolari. Alcune volte si può incorrere in qualche confusione. Per esempio, se decidiamo che ac.com deve andare nella white-list, bisogna stare attenti perché alla stessa stregua ci andranno anche espressioni del tipo billing.ac.com, ed è ovvio, o anche, ed è meno evidente, drac.complete.viagra.sales.com (perché ac.com viene riconosciuto in mezzo alla stringa...).

Per evitare tutto ciò, dobbiamo usare le espressioni RegEx appropriate, comprendenti tutti i segni ^ e $ necessari per "forzare" l'inizio e la fine della stringa. Ovviamente quando ciò è possibile.

Tutto ciò va impostato nel file priolist.mfp, dove all'inizio di ogni espressione regolare dobbiamo mettere un + o un – per indicare rispettivamente se l'espressione indica una regola da white-list o da black-list.

Linguaggio C usiamo i SOCKET per CONNESSIONI tra PC e SERVER



Con i socket si possono stabilire connessioni tra due o più computer, aclient e server. Ecco come fare per sperimentarne la programmazione in linguaggio C

I socket non è altro che una procedura che permette a un processo di comunicare con un altro: ma l'importante è che i due processi possono risiedere su macchine diverse. Quindi, in poche parole, con i socket si possono stabilire connessioni tra due o più computer, client e server. In questo articolo vogliamo gestire i socket dalla parte del client e per fare ciò partiamo con l'idea di creare un socket per un client che manda e-mail.

Alla base

Ogni volta che mandiamo una e-mail dal nostro browser di posta - Outlook, K-Mail, eccetera - non facciamo altro che stabilire una connessione con un server (di solito il server smtp.provider.it).

Avvenuta la connessione, inviamo al server alcuni comandi che lui saprà riconoscere e quindi interpretare, permettendogli così anche di inviare la nostra e-mail. Naturalmente il server esegue con successo i comandi del nostro client perché tutti e due utilizzano il protocollo SMTP (Simple Mail Transfer Protocol): se per caso il client invia un istruzione che il server non sa riconoscere, significa che uno dei due programmi (client o server) non funziona correttamente.

Creiamo il nostro socket

Innanzitutto inseriamo i file header (*.h) per gestire le funzioni dei socket sotto UNIX:

```
#include <netdb.h>
#include <netinet/in.h>
#include <string.h> /* per memset */
#include <sys/types.h>
#include <sys/socket.h>
```

Fatto questo utilizziamo la chiamata del socket:

```
int socket (int dominio, int tipo, int protocollo);
```

Questa funzione restituisce -1 se si verifica un errore nella creazione, altrimenti restituisce il descrittore del socket. I parametri in ingresso sono tre:

dominio: restituisce un intero, e non è altro che la famiglia di protocolli deve essere utilizzata.
Noi utilizzeremo la famiglia dei protocolli IPv4 (PF_INET);

tipo: il tipo di protocollo da utilizzare. Siccome dobbiamo stabilire una connessione tra un client e un server utilizzeremo il tipo TCP (SOCK_STREAM);

protocollo: impone al sistema di utilizzare un protocollo. Utilizzeremo il valore 0, in modo che sia il sistema stesso a scegliere il protocollo più adatto.

A questo punto per creare il nostro socket basterà scrivere:

```
int sd = socket (PF_INET, SOCK_STREAM, 0);
```

Inseriamo i dati relativi al server

Adesso dobbiamo inserire i dati relativi al nostro server SMTP (server e porta); per fare questo dichiariamo la seguente variabile:

```
struct sockaddr_in client;
```

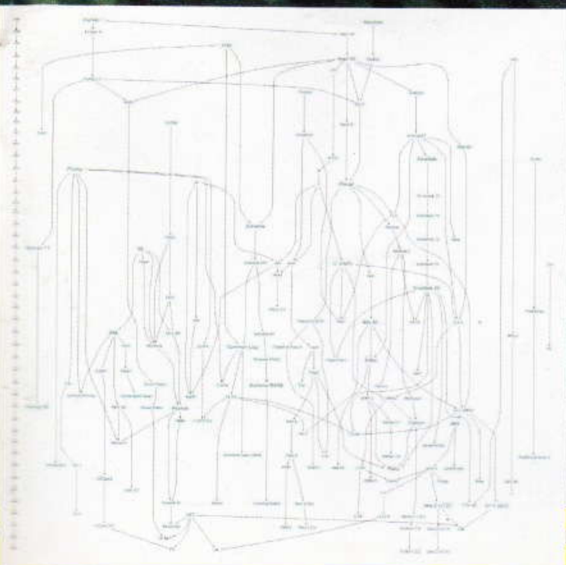
Non abbiamo fatto altro che dichiarare un record (client) di tipo sockaddr_in. Dopodiché azzerriamo, per sicurezza, tutti i campi della variabile client:

```
memset (&client, '\x0', sizeof (client)); /* memset(...) è contenuta nel header <string.h> */
```

A questo punto creiamo un'altra variabile speciale, in cui andremo a mettere l'indirizzo del nostro server:

```
struct hostent *server;
server = gethostbyname ("smtp.provider.it"); /* nome del provider (es: smtp.tin.it) */
```

Quindi, con le prossime tre istruzioni, raggrupperemo tutto quanto nel record client, settando i campi appropriati:



```
client.sin_family = PF_INET;
client.sin_port = htons (25); /* 25 è di default, la porta dei server SMTP */
client.sin_addr.s_addr = ((struct in_addr*)(server -> h_addr)) -> s_addr; /* settiamo l'indirizzo del server */
```

Connettiamoci al server

```
int connect (int descrittore, struct sockaddr *serv_addr, int lungh_ind);
```

Questa chiamata ci permette di connetterci al server; i suoi parametri sono:

descrittore: il nostro socket (sd);
serv_addr: l'indirizzo della struttura di tipo struct sockaddr *, che contiene l'indirizzo del server;
lungh_ind: la lunghezza effettiva della struttura che contiene l'indirizzo.

La funzione restiuisce -1, se non siamo riusciti a conneterci al server. La funzione nel nostro programma verrà quindi trasformata in:

```
connect (sd, (struct sockaddr*)&client, sizeof (client));
```

Invio e ricezione dei dati

Quando connessi, non ci rimane altro che inviare i famosi comandi che il server SMTP riesce a capire e per farlo serve la funzione:

```
int send (int descrittore, const void *msg, int len, unsigned int flags);
```

I parametri sono:

descrittore: il nostro socket (sd).
msg: la nostra istruzione.
len: la lunghezza della nostra istruzione.
flags: è un attributo, di solito è posto uguale a 0.

La funzione restituisce il numero di byte trasmessi.

Per ricevere invece i dati dal server utilizziamo la funzione:

```
int recv (int descrittore, void *buf, int len, unsigned int flags);
```

che possiamo intuire possiede parametri uguali alla send. Naturalmente la funzione restiuisce il numero di byte ricevuti.

Codice

Naturalmente ora bisogna implementare il codice, che come abbiamo già capito è del tipo:

```
char buffer[4000];
send (sd, "HELO provider", sizeof ("HELO provider") + 1, 0);
if (recv (sd, buffer, sizeof (buffer) + 1, 0) != 0)
    printf ("%s", buffer);
```

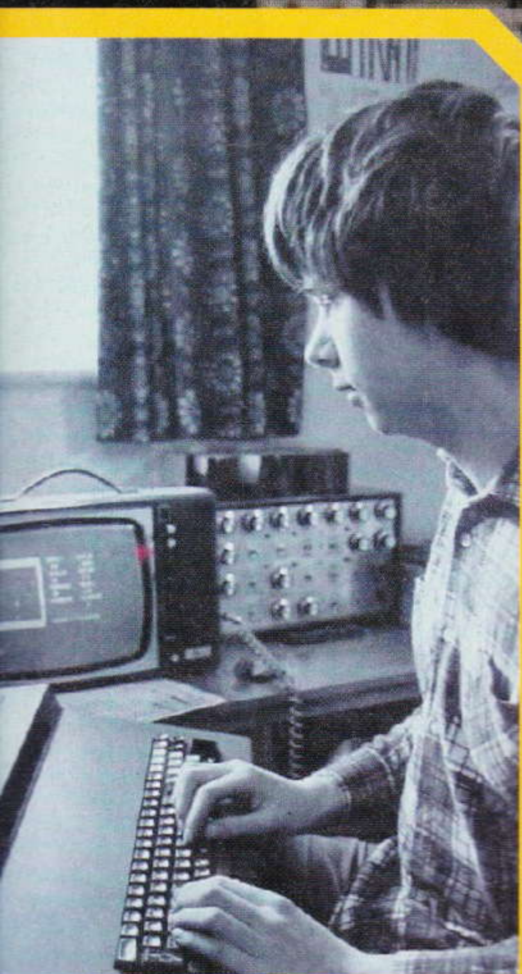
eccetera...
Ai più ardimentosi la stesura del programma!

Ricordiamoci che in C tutte le dichiarazioni delle variabili devono essere dichiarate prima del codice, quindi buffer, client, e così via vanno dichiarate all'inizio.
Se non conosciamo troppo bene il protocollo SMTP, leggiamoci il manuale di Lord Shiva che è reperibile in qualsiasi sito Hacking (per esempio: http://www.zaratustra.it/shiva.htm). E ora: sotto con la fantasia!

michele
michele.facchin@virgilio.it

I COMPUTER che

Non tutti gli hacker sono diventati famosi, ma molti di loro hanno contribuito alla storia dei computer. Chaos 1 e Chaos 2 sono stati costruiti da un hacker ingegnoso nientemeno che dal 1977 in avanti. A leggere le specifiche c'è da ridere!



TUTTI GLI ACCESSORI DI CHAOS 1

- Interfaccia per registratore a cassette audio, sui venivano registrati i programmi.
- Scheda video.
- Scheda di RAM da 16K.
- Seconda scheda di RAM da 16K.
- Coprocessore numerico e scheda da 256K + 2K di RAM.
- Lettore di floppy disk da 5"25.
- Unità di generazione di suono e codice Morse.
- Stampante.
- Tastiera via porta parallela

Oggi DJ Greaves tiene conferenze di Computer Science all'Università di Cambridge negli Stati Uniti. Ma nel 1977 era un ragazzo intraprendente che ricevette in regalo un microprocessore 2650 di Signetics, a otto bit. Lui ci ha costruito intorno un computer, anzi due: Chaos 1, dal 1977, e Chaos 2, evoluzione del primo, a partire dal 1983. Il computer era fatto di legno, con una tastiera di recupero montata di fronte, sotto banchi di LED, e l'alimentatore sul retro. I LED servivano a mostrare lo stato dei 15 bit del bus A, gli otto bit del bus D e gli otto bit dei registri del processore. Decisamente i Pentium erano di là da venire, tanto è vero che i dati venivano scritti in memoria tramite accesso diretto fermando il processore, che veniva riavviato quando i dati erano in memoria, pronti per l'elaborazione. Sempre sul retro della macchina comparivano i connettori per le espansioni del computer.

La scheda video

La prima scheda video di Chaos 1, costruita intorno a un controller video capace di mostrare ben 16 righe di testo ASCII (niente grafica bitmap, dove ogni pixel è singolarmente gestibile) per un massimo di 80 caratteri ciascuna, in monocromatico. Il numero di caratteri per riga poteva essere variato girando una manopola e i caratteri totali mostrabili erano 128, ognuno in due stati: maiuscolo e minuscolo.

Non era supportato un cursore e quindi non c'era editing a tutto schermo; se si sbagliava a digitare una riga bisognava



▲ ***Chaos 1 era fatto di legno, con tasti presi da altri computer e altri componenti recuperati qua e là.***

hanno fatto la STORIA

cancellare tutti i caratteri fino all'errore e ridigitare pazientemente. La scheda era collegata all'unità centrale da una porta seriale RS-232 a 9.600 bit per secondo e proiettava la schermata su un televisore a valvole da 12 pollici.

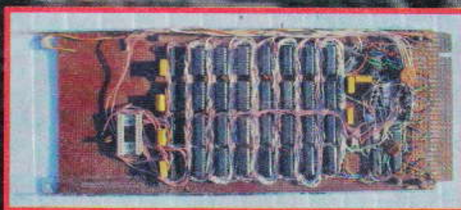
Il lettore di floppy

Nel 1980 Chaos 1 venne dotato di un lettore di floppy disk, come si vede piuttosto artigianale. Ogni floppy aveva la capacità di 300K, ottenuti dividendo la superficie in 35 tracce da otto settori ciascuna, 256 byte per ciascun settore.

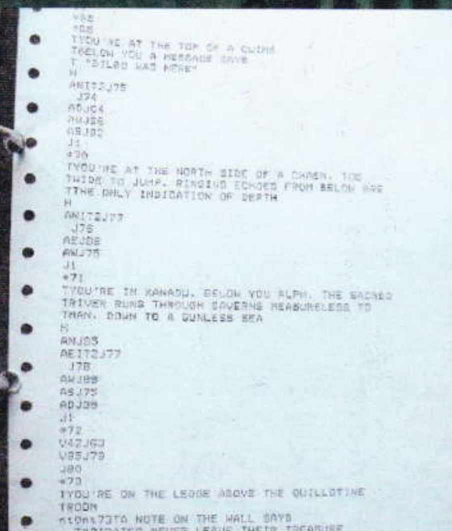
Sono curiosi gli interruttori posti sul frontale. Servivano a consentire la formattazione dei floppy, cambiare floppy e cambiare sistema di divisione in settori del floppy. Ma prima del 1980 la memoria di massa di Chaos 1 consisteva nel registratore a cassette. La velocità di registrazione era di 30 o 600 bit per secondo.

La RAM

A quei tempi una persona non ricca non poteva permettersi di comprare RAM in grandi quantità e quindi i chip venivano aggiunti alla scheda man mano che si compravano. La memoria principale di Chaos 1 consisteva in due schede da 16K l'una, corrispondenti alla massima quantità di RAM gestibile dal processore.



▲ *Una scheda da 16K di RAM delle due usate da Chaos 1. I chip venivano aggiunti quando c'erano i soldi per comprarli.*



```
TYOU'RE AT THE TOP OF A CLIMB
TBELOW YOU A MESSAGE SAYS
T "BILBO WAS HERE"
H
ANIT2J75
 J74
ADJC4
AWJ26
ASJ02
J1
*70
TYOU'RE AT THE NORTH SIDE OF A CHASM, TOO
TWIDE TO JUMP. RINGING ECHOES FROM BELOW ARE
TTHE ONLY INDICATION OF DEPTH
H
ANIT2J77
 J76
AEJ08
AWJ75
J1
*71
TYOU'RE IN XANADU. BELOW YOU ALPH, THE SACRED
TRIVER RUNS THROUGH CAVERNS MEASURELESS TO
TMAN, DOWN TO A SUNLESS SEA
H
ANJ03
AEIT2J77
 J78
AWJ09
ASJ75
ADJ39
J1
*72
V42J63
V35J79
J80
*73
TYOU'RE ON THE LEDGE ABOVE THE GUILLOTINE
TROOM
TA NOTE ON THE WALL SAYS
T"PIRATES NEVER LEAVE THEIR TREASURE
```

▲ *Un brano del codice in assembly di CARCE, un adventure game. Su Chaos 1 si poteva persino giocare!*

Chaos 2

Nel 1983 nacque Chaos 2, il successore di Chaos 1. Aveva un proprio chassis e somigliava a un computer assai più del suo predecessore, addirittura con un hard disk da venti megabyte, 128K di RAM, due processori 2650 e un 8088 Intel, e il collegamento a un sintetizzatore polifonico analogico, pilotato da un processore Z80 a otto bit.



Vista da lontano di Chaos 1. A un millesimodella potenza di un computer di oggi, occupava praticamente due scrivanie

Complimenti, Mr. Greaves

A vedere queste foto viene da ringraziare di essere nel XXI secolo. Ma abbiamo anche la sensazione che DJ Greaves, da giovane, si sia divertito parecchio con il suo computer.



BASTA

Sentire il pilota che parla con la torre di controllo: basta una comune radiolina. Ecco come possiamo trasformare una radio FM in uno scanner

Spingere un programma, un circuito, una macchina oltre le funzioni/prestazioni per le quali è stato progettato rappresenta certamente l'aspetto più stimolante della filosofia hacker. In quest'ottica, possiamo spingere "oltre" anche una comune radio operante sulla banda 88-108 MHz, fino a consentirci l'ascolto di frequenze "non previste": basta intervenire sui componenti giusti.

Da un punto di vista tecnico possiamo riassumere il funzionamento di un ricevitore in questo modo:
- **uno stadio ricevente** (antenna e circuito di accordo)
- **un oscillatore locale**
- **un miscelatore**
- **un rivelatore**

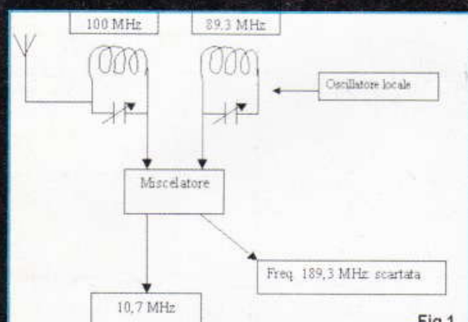
Ciò che interessa per il nostro scopo sono i primi due stadi del sistema: il circuito di accordo e l'oscillatore locale.

Un po' di tecnica

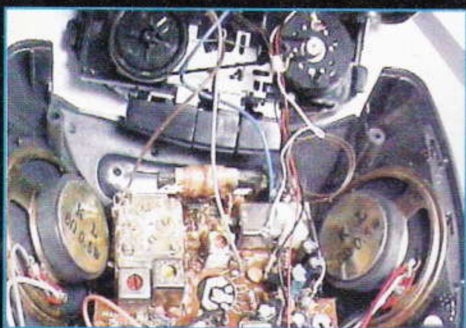
Premesso che il circuito di accordo e l'oscillatore locale sono due sistemi che oscillano a frequenze leggermente diverse condividendo un condensatore variabile, viene da domandarci per quale motivo dobbiamo intervenire su entrambi e non solo sullo stadio iniziale. Bene, la scelta di un simile schema circuitale è dettata dal fatto che il segnale ricevuto deve essere amplificato per consentirne la successiva "decodifica". Per questo motivo, dovendo accordare l'amplificatore su una frequenza ben precisa (al fine di limitare al massimo le interferenze delle frequenze vicine) è stato creato un circuito di conversione nel modo seguente:

-supponiamo di voler ricevere una emittente che trasmette sui 100MHz, il circuito di accordo dell'antenna sarà sintonizzato proprio su quella frequenza, mentre l'oscillatore locale risulterà sintonizzato su una frequenza inferiore (di 10,7 MHz per motivi tecnici).
In questo modo, poiché il condensatore variabile è comune per entrambi, al variare della frequenza di uno stadio, varia anche l'altra ottenendo sempre una differenza di 10,7 MHz.
Tale frequenza (di sottrazione) è ottenuta dallo stadio miscelatore, sistema caratterizzato dal fatto che accetta due frequenze in ingresso restituendone altre due pari alla somma ed alla differenza di quelle in ingresso (fig.1). A questo punto, scartata la frequenza di addizione, non resta che tarare il funzionamento degli stadi successivi per 10,7 MHz e il gioco è fatto.
Quanto descritto non è certamente il massimo in termini tecnici, ma basta per capire il funzionamento di base di un ricevitore e, finalmente, pensare a quali modifiche siano possibili.

UNA RADIOLINA



▲ Dobbiamo intervenire sulle due bobine: quella di sintonia e quella dell'oscillatore locale.



▲ Una vista interna della radio modificata

Lo stadio di accordo e l'oscillatore locale

Lo stadio di accordo e l'oscillatore locale possono essere ridotti schematicamente a un condensatore variabile e una bobina ciascuno, il loro funzionamento può essere descritto come un circuito nel quale la corrente alternata viaggia avanti e indietro con una frequenza che varia in base alla capacità del condensatore e all'induttanza della bobina. Tra i due componenti, quello modificabile con maggiore semplicità è certamente la bobina, costituita da un filo di rame smaltato di circa 0,5 mm di diametro, avvolto (di norma) su cinque spire, senza nucleo ferroso. Questa bobina, determina la frequenza di oscillazione grazie alla sua "induttanza", valore che varia in base al numero di spire e allo spazio tra ciascuna di esse (in realtà l'induttanza varia anche in base al diametro del filo e al materiale sul quale questo viene avvolto, ma a noi basteranno gli elementi descritti). Considerato che la frequenza diminuisce al diminuire dell'induttanza e che questa diminuisce in questi due casi:

- **diminuzione delle spire;**
- **aumento dello spazio tra le spire;**

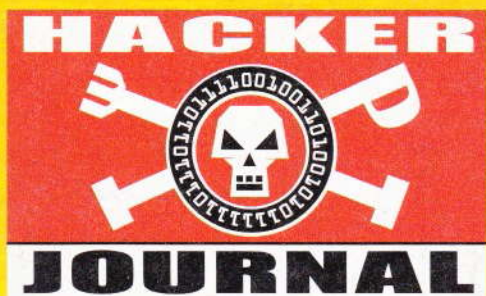
si giunge alla naturale conseguenza per la quale:

diminuzione delle spire
+
piccole variazioni di spaziatura (per la taratura fine)
=
incremento della frequenza di ricezione!

Dunque, secondo il nostro (seppure approssimativo) ragionamento, per elevare la frequenza di ricezione di circa 20 MHz, dovremmo ridurre il numero di spire di circa 1/5 (dato che la banda centrale della radio FM è di circa 100 MHz) e quindi dovremmo portare a quattro il numero di spire della bobina.
Per fare quanto detto dobbiamo utilizzare un saldatore a stagno e procedere alla "dissaldatura" delle due bobine, dopodiché potremo accorciare il filo di rame smaltato di quanto serve per eliminare una spira (per ciascuna bobina) e avendo cura di lasciare un po' di filo in più per poterlo saldare nuovamente alla piastrina del circuito stampato.

Perché sia possibile saldare il filo, è necessario che "grattiamo" via la smaltatura per la parte che dovrà essere saldata. Consigliamo di utilizzare una matita o un chiodo per ridare la forma alla bobina, qualora si fosse rovinata. Una volta eseguite le modifiche e saldate le due bobine, si può accendere la radio e iniziare la taratura. Il modo migliore consiste nel ricercare pazientemente una comunicazione cercando di comprenderne la provenienza.
Fatto ciò si potrà stabilire la frequenza reale del messaggio ricevuto così da poter iniziare una sorta di conversione della scala parlante della nostra radiolina: ad esempio, se ascoltiamo un aereo possiamo risalire alla frequenza assegnata all'aeroporto più vicino.
Per avere maggiori probabilità di ascoltare qualche comunicazione, qualora la nostra frequenza "obiettivo" sia quella dell'aviazione, consigliamo di attendere il passaggio di un elicottero o un aereo e cominciare una scansione della sintonia, lenta e costante, fino alla ricezione della voce un po' gracchiante del pilota che comunica con la torre di controllo.
Ricevuta qualche comunicazione, potremo anche procedere a una migliore sintonia aumentando o diminuendo la spaziatura tra le spire della sola bobina nello stadio di accordo (per riconoscerla basti sapere che agendo sulla spaziatura di questa varierà l'intensità del segnale ricevuto, mentre se agissimo sull'altra bobina il segnale sparirebbe a causa della variazione di frequenza dell'oscillatore locale). Buon ascolto.

AlessandroBadiale-M0t0Gu221

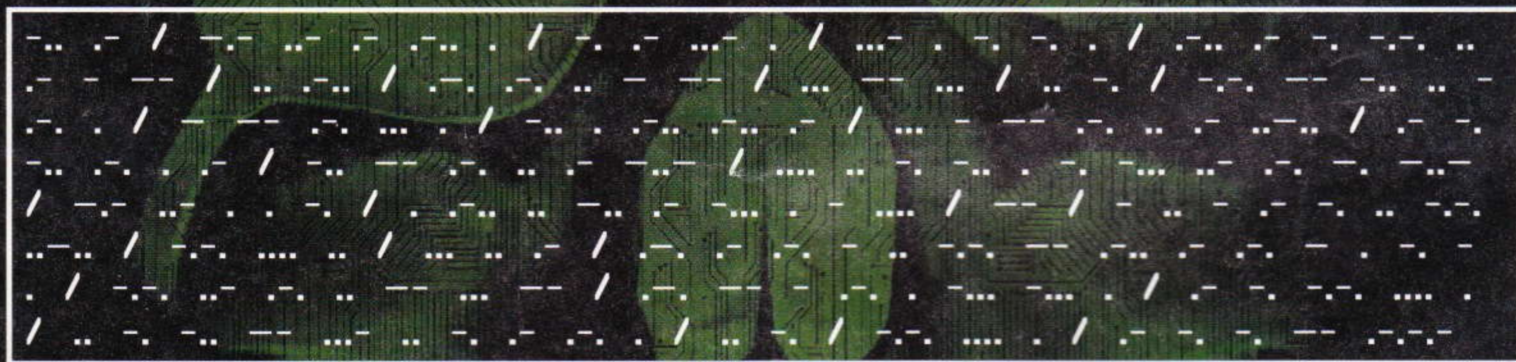


IL PROSSIMO NUMERO IN EDICOLA IL 20 maggio 2004!

CYBERENIGMA

Ecco una nuova sfida per il nostro Cyberenigma!

Sotto appare una domanda; è scritta in un alfabeto molto in voga nel secolo scorso, che nacque per sfruttare l'invenzione del telegrafo.



Sintassi: gli spazi separano le lettere. Le barre (/) separano le parole.

✪ **Per tutti:** di che alfabeto si tratta?
✪✪ **Per esperti:** Che cosa c'è scritto?
✪✪✪ **Per geni:** Quali sono le risposte?
✪✪✪✪ **Per super hacker:** Chi riesce a scrivere un programma di traduzione automatica da questo alfabeto nel nostro, e magari viceversa?

Per chi si sta disperando:
Su Internet si trova anche un motore già fatto, che traduce all'istante in un senso o nell'altro. A chi ci scrive chiedendo soccorso risponderemo. Ma il vero hacker trova molta più soddisfazione nel trovare la risposta da sé!

Alla prossima!